Supreme Court, U.S.
FILED

96 595 OCT 15 1996

No. OFFICE OF THE CLERK

In the Supreme Court of the United States

OCTOBER TERM, 1996

JANET RENO, ATTORNEY GENERAL OF THE UNITED STATES, APPELLANT

v.

JOE SHEA

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF NEW YORK

JURISDICTIONAL STATEMENT

WALTER DELLINGER
Acting Solicitor General

FRANK W. HUNGER
Assistant Attorney General

EDWIN S. KNEEDLER
Deputy Solicitor General

IRVING L. GORNSTEIN
Assistant to the Solicitor General

BARBARA L. HERWIG
JACOB M. LEWIS
Attorneys

Department of Justice
Washington, D.C. 20530-0001
(202) 514-2217

102 pp

QUESTIONS PRESENTED

1. Whether the federal criminal prohibition against "knowingly" using an "interactive computer service" to send to "a specific person or persons under 18 years of age," any material "that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs," 47 U.S.C. 223(d)(1)(A), is unconstitutional on its face.

2. Whether the federal criminal prohibition against "knowingly" using an "interactive computer service" to "display in a manner available to a person under 18 years of age," any material "that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs," 47 U.S.C. 223(d)(1)(B), is unconstitutional on its face.

3. Whether the federal criminal provision that forbids a person from knowingly permitting the use of a telecommunications device under such person's control to be used to violate either of the two preceding prohibitions, 47 U.S.C. 223(d)(2), is unconstitutional on its face.

TABLE OF CONTENTS

	Page
Opinion below	1
Jurisdiction	1
Constitutional and statutory provisions involved	1
Statement	2
Discussion	9
Conclusion	13
Appendix A	1a
Appendix B	76a
Appendix C	78a

TABLE OF AUTHORITIES

Cases:

American Civil Liberties Union v. *Reno*, 929 F. Supp. 824 (E.D. Pa. 1996), appeal pending, No. 96-511	3, 13
Denver Area Educational Telecommunications Consortium, Inc. v. *FCC*, 116 S. Ct. 2374 (1996)	10
FCC v. *Pacifica Foundation*, 438 U.S. 726 (1978)	7
Miller v. *California*, 413 U.S. 15 (1973)	10

Constitution and statutes:

U.S. Const. :	
Amend. I	1, 2, 7, 10
Amend. V (Due Processs Clause)	10
Communications Act of 1934, 47 U.S.C. 608	11
Telecommunications Act of 1996, Pub. L. No. 104-104, Tit. V, 110 Stat. 56 (Communications Decency Act of 1996)	2, 4
§ 502, 110 Stat. 133	1-2, 5, 78a
47 U.S.C. 223(a)(1)(B)	6, 12
47 U.S.C. 223(a)(2)	6, 11, 12

Statutes—Continued: Page

§ 502(2), 110 Stat. 133 ..... 5, 6, 80a
47 U.S.C. 223(d) 2, 5, 6, 7, 8, 9, 10
47 U.S.C. 223(d)(1) 11
47 U.S.C. 223(d)(1)(A) 5, 10, 11
47 U.S.C. 223(d)(1)(B) 5, 10, 11
47 U.S.C. 223(d)(2) 6, 11
47 U.S.C. 223(e)(5) 8
47 U.S.C. 223(e)(5)(A) 6, 9
47 U.S.C. 223(e)(5)(B) 6, 10
§ 509, 110 Stat. 138 4
47 U.S.C. 230(a)(1) 4
47 U.S.C. 230(a)(3) 4
§ 561(a), 110 Stat. 142 7
§ 561(b), 110 Stat. 143 2

Miscellaneous:

141 Cong. Rec. (daily ed. June 9, 1995):
p. S8087 5
p. S8088 5
p. S8089 5

In the Supreme Court of the United States

OCTOBER TERM, 1996

No.

JANET RENO, ATTORNEY GENERAL OF THE UNITED STATES, APPELLANT

v.

JOE SHEA

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF NEW YORK

JURISDICTIONAL STATEMENT

OPINION BELOW

The opinion of the three-judge district court (App., *infra*, 1a-75a) is reported at 930 F. Supp. 916.

JURISDICTION

The judgment of the district court was entered on July 29, 1996. A notice of appeal was filed on August 15, 1996. App., *infra*, 76a-77a. The jurisdiction of this Court is invoked under Section 561(b) of the Communications Decency Act of 1996, Pub. L. No. 104-104, 110 Stat. 143, and 28 U.S.C. 1253.

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

The First Amendment provides that "Congress shall make no law * * * abridging the freedom of speech." Section 502 of the Communications Decency

Act of 1996, Pub. L. No. 104-104, 110 Stat. 133, appears in the appendix to the jurisdictional statement. App., *infra*, 78a-85a.

STATEMENT

This case involves a constitutional challenge to provisions of the Communications Decency Act of 1996 (CDA) that prohibit the use of "interactive computer services" to disseminate "patently offensive" sexually explicit materials to children under 18 years of age. 47 U.S.C. 223(d). The term "interactive computer services" includes, but is not limited to, the global computer network known as the "Internet."

Appellee, the editor-in-chief, publisher and part-owner of an electronic newspaper distributed over the Internet, filed suit in the United States District Court for the Southern District of New York, asserting that Section 223(d)'s restrictions on patently offensive computer communications violate the First Amendment. The suit was heard by a three-judge court, which held the restrictions unconstitutional on their face and issued a preliminary injunction against their enforcement. The court held that Section 223(d)'s restrictions are not unconstitutionally vague. The court concluded, however, that the prohbitions are unconstitutionally overbroad because they deter many persons from engaging in constitutionally protected adult-to-adult communications. Pursuant to Section 561(b) of the CDA, which authorizes a direct appeal to this Court as of right in such circumstances, the Attorney General has appealed from the preliminary injunction.

Prior to the decision in this case, a three-judge court in the United States District Court for the Eastern District of Pennsylvania had also issued a

preliminary injunction against enforcement of the CDA's restrictions on patently offensive communications. *American Civil Liberties Union (ACLU)* v. *Reno*, 929 F. Supp. 824 (1996). The Attorney General has appealed from that preliminary injunction, and the jurisdictional statement in that case was filed on September 30, 1996. *Reno* v. *American Civil Liberties Union* (*ACLU*), No. 96-511.

1. As we explain in our jurisdictional statement in *ACLU* (at 3-6) (a copy of which we are providing to appellee), the Internet is a global network of interlinked computers that is used both for communication and for information retrieval. As many as 40 million people use the Internet today, and that figure is expected to grow to 200 million by the year 1999. App., *infra*, 13a.

There are various ways to obtain a connection to the Internet. For example, national commercial online services, such as America Online, provide an Internet connection as part of the monthly fee they charge their subscribers for access to their own computer networks. App., *infra*, 14a. "Internet service providers" also offer access (again ordinarily for a fee) to computers that are linked to the Internet. *Id.* at 13a. In addition, educational institutions often provide Internet access to students and faculty through computers located on campus, and some businesses provide their employees with Internet access through office networks. *Id.* at 12a-13a.

Communication over the Internet also takes a variety of forms. One of the most common is through electronic mail (e-mail). Using e-mail, an individual can send an electronic message to one or more specific persons. App., *infra*, 15a-16a. People can also use automatic mailing list programs (such as listserv) to

send messages on a particular topic (such as health care) that are then automatically distributed via e-mail to those who have subscribed to the mailing list. *Id.* at 16a. Information can also be exchanged through newsgroups. *Id.* at 17a. Like listserv users, newsgroup users ordinarily exchange information on specific topics. Unlike listserv users, however, newsgroup users do not ordinarily have to subscribe in advance; instead, they usually can obtain access to the information at any time. *Ibid.* Persons can also use the Internet to communicate in "real time." Programs such as "talk" permit one-to-one communication; programs such as "Internet Relay Chat" permit communication among several persons. *Id.* at 18a.

The Internet can also be used to retrieve information stored on remote computers. App., *infra*, 18a. The most well-known method of doing that is through the "World Wide Web," which uses a formatting language that permits the display of documents containing text, images, and sound. *Id.* at 20a. The Web's language also permits documents to include "links" to other Internet documents, so that with the click of a computer mouse a person can move from one document to another even if the documents are stored on computers in different parts of the world. *Ibid.* In addition, "search engines," such as Altavista and Yahoo, allow persons to comb the Web for sites that contain certain categories of information or specified key words. *Id.* at 21a.

2. Congress understood the extraordinary educational and informational value of the Internet. See Telecommunications Act of 1996, Pub. L. No. 104-104, § 509, 110 Stat. 138 (to be codified at 47 U.S.C. 230(a)(1) and (3)). Congress was concerned, however, that without "some basic rules of the road," the

increase in the availability and easy accessibility of sexually explicit materials facilitated by the Internet would result in harm to children. 141 Cong. Rec. S8087 (daily ed. June 9, 1995) (remarks of Sen. Exon). As Section 223(d)'s principal sponsor explained, "[t]he computer is a wonderful device for arranging, storing, and making it relatively easy for anyone to call up information or pictures on any subject they want," 141 Cong. Rec. S8089 (daily ed. June 9, 1995) (statement of Sen. Exon), but that same technology allows sexually explicit materials, including "the worst, most vile, [and] most perverse pornography," to be "only a few click-click-clicks away from any child." *Id.* at S8088.

b. Section 502(2) of the CDA responds to the increasing availability of sexually explicit materials through computers by adding two distinct restrictions on the use of "interactive computer services," both contained in 47 U.S.C. 223(d). See Pub. L. No. 104-104, § 502, 110 Stat. 133-134. The first prohibits the knowing use of an interactive computer service "to send to a specific person or persons under 18 years of age" material "that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs." 110 Stat. 133-134 (to be codified at 47 U.S.C. 223(d)(1)(A)). The second prohibits the use of an interactive computer service "to display [such material] in a manner available to persons under 18 years of age." 110 Stat. 134 (to be codified at 47 U.S.C. 223(d)(1)(B)). Complementing those two restrictions, Section 502(2) also prohibits any person from "knowingly permit[ting] any telecommunications facility under [that person's] control to be used for any activity prohibited by" the other

prohibitions. 110 Stat. 133, 134 (to be codified at 47 U.S.C. 223(d)(2)). Persons who violate those prohibitions are subject to criminal fines and/or imprisonment for not more than two years. .Pub. L. No. 104-104, § 502(2), 110 Stat. 134, 135 (to be codified at 47 U.S.C. 223(d)).[1]

Section 502(2) provides a "defense to prosecution" for those persons who have restricted access to their communications "by requiring use of a verified credit card, debit account, adult access code, or adult personal identification number." 110 Stat. 134 (to be codified at 47 U.S.C. 223(e)(5)(B)). A defense is also available to those who have "taken, in good faith, reasonable, effective, and appropriate actions under the circumstances to restrict or prevent access by minors" to indecent or patently offensive communications, "including any method which is feasible under current technology." 110 Stat. 134 (to be codified at 47 U.S.C. 223(e)(5)(A)).

3. Appellee is the editor-in-chief, publisher and part owner of the *American Reporter*, a daily electronic newspaper distributed to subscribers by e-mail and made available on the World Wide Web. App., *infra*, 1a. On February 8, 1996, the day the President signed the CDA into law, appellee filed suit in the

---

[1] Section 502 also amends 47 U.S.C. 223(a)(1)(B) to forbid any person from using a "telecommunications device" to "knowingly * * * make[], create[], or solicit[], and * * * initiate the transmission of" any communication "which is obscene or indecent, knowing that the recipient of the communication is under 18 years of age." 110 Stat. 133. That provision, and its counterpart restriction on permitting the use of a telecommunications device by another to do the same thing, 47 U.S.C. 223(a)(2), are at issue in the *ACLU* case, but they are not at issue in this case.

United States District Court for the Southern District of New York against the Attorney General to challenge Section 223(d)'s restrictions on patently offensive sexually explicit communications. App., *infra*, 2a-3a. Appellee alleged that those restrictions are unconstitutionally vague and overbroad in violation of the First Amendment. *Id.* at 3a.

A three-judge district court convened under Section 561(a) of the CDA, 110 Stat. 142, rejected appellee's contention that Section 223(d)'s restrictions are unconstitutionally vague. The court observed that Section 223(d) "essentially codifies the FCC['s] definition of indecency sustained in a particular factual context" by this Court in *FCC* v. *Pacifica Foundation*, 438 U.S. 726 (1978). App., *infra*, 37a. It noted, moreover, that several courts of appeals have read the *Pacifica* opinion to foreclose vagueness challenges to the FCC's indecency definition as applied to broadcasting, cable television, and commercial telephone messages. *Id.* at 37a-38a. In light of those precedents, the court concluded that appellee had not demonstrated "a likelihood of success on his claim that the incorporation of a virtually identical verbal formula into § 223(d) renders that statute fatally vague." *Id.* at 38a. The court expressly rejected the contrary conclusion reached by the court in the *ACLU* case. *Id.* at 39a.

Agreeing with the court in *ACLU*, however, the court in this case held that the restrictions on patently offensive communications in Section 223(d) are unconstitutionally overbroad. The court acknowledged that "sexually explicit content is available on the Internet through almost any form of Internet communication," App., *infra*, 26a, and it assumed that the government has a "compelling" interest in re-

stricting children's access to patently offensive sexually explicit material. *Id.* at 52a. The court nonetheless determined that, "for the vast majority of applications and services available on the Internet, a user has no way of communicating or making available patently offensive content with certainty that the content will not reach a person under eighteen years of age." *Ibid.* The court therefore concluded that the "only way for a content provider to comply with § 223(d), standing alone, would be to refrain from transmitting any indecent content." *Id.* at 53a. That result would "unquestionably be unconstitutional," the court reasoned, because communications that are indecent but not obscene are constitutionally protected for adults. *Ibid.*

The court concluded that Section 223(e)(5)'s defenses to prosecution do not save the constitutionality of Section 223(d)'s restrictions. The court acknowledged that commercial providers of content on the World Wide Web could restrict their material to adults by requiring the use of a verified credit card as a condition of access. App., *infra*, 55a-56a. But the court found that credit card or other forms of adult verification would be "extremely costly" for noncommercial content providers and "possibly" some commercial providers. *Id.* at 56a-57a. The court also recognized that there are companies, such as "Adult Check" and "Validate," that are in the business of providing adult verification services, often at no cost to an Internet content provider. *Id.* at 33a, 57a. The court nevertheless concluded that it would be unduly burdensome for some commercial and noncommercial content providers to employ adult verification services to screen access to their sites, because such

services are currently used by adult sites offering pornographic images. *Id.* at 57a.

The court also determined that Section 223(e)(5)(A) of the CDA, which provides a defense to prosecution for those persons who take "in good faith, reasonable, effective and appropriate actions" to restrict minors' access to indecent materials, "does not provide a safe harbor in a substantial number of circumstances." App., *infra*, 60a-61a. The court concluded that identifying material as indecent through a tag that could be blocked by browsers and screening software is not currently effective in restricting access to children. *Id.* at 61a-66a. The court also rejected options such as closed mailing lists and limited newsgroups that screen for age on the ground that they are too costly and burdensome. *Id.* at 68a-69a. Finally, the court refused to uphold Section 223(d) as applied to commercial content providers, because the statute does not distinguish between commercial and non-commercial providers. App., *infra*, 71a-74a.

Based on its view that the CDA's restrictions on patently offensive sexually explicit computer communications are facially unconstitutional, the court issued a preliminary injunction preventing the government from "initiating any investigation or prosecution under § 223(d), to the extent that such investigation or prosecution is based upon the alleged display or transmission of indecent but not obscene material." App., *infra*, 75a.

DISCUSSION

1. The court below correctly determined that the restrictions on patently offensive sexually explicit computer communications contained in Section 223(d) are not unconstitutionally vague. As we explain in

our jurisdictional statement in *ACLU* (at 17-19), this Court's rejection of vagueness challenges to analogous prohibitions in *Miller* v. *California*, 413 U.S. 15 (1973), and *Denver Area Educational Telecommunications Consortium, Inc.* v. *FCC*, 116 S. Ct. 2374 (1996), demonstrate that Section 223(d)'s restrictions give sufficient warning concerning the core of what they prohibit to satisfy the First Amendment and the Fifth Amendment Due Process Clause.

The court erred, however, in holding that Section 223(d)'s indecency restrictions are facially overbroad. The premise of the court's holding was that Section 223(d)'s restrictions interfere with adult-to-adult communications in a substantial number of cases. But as we explain in our jurisdictional statement in *ACLU* (at 21), that concern is not significantly implicated by Section 223(d)(1)(A), which prohibits the "knowing[]" use of an "interactive computer service to send [patently offensive material] to a specific person or persons under 18 years of age." 47 U.S.C. 223(d)(1)(A). To comply with that provision, adults need not refrain from communicating patently offensive material to other adults; they need only refrain from disseminating such material to persons they know to be under 18 years of age.

Section 223(d)(1)(B), which prohibits the "knowing[]"use of an interactive computer service "to display [patently offensive material] in a manner available to a person under 18 years of age," raises more difficult questions. But the CDA provides a defense to prosecution when the user restricts access through a verified credit card or an adult ID, 47 U.S.C. 223(e)(5)(B), or otherwise takes "good faith, reasonable, effective and appropriate" steps to prevent children from obtaining access to the material. As we

explain in our jurisdictional statement in *ACLU* (at 21-25), those statutory defenses are available in a wide range of cases, and the CDA leaves open a number of avenues for adult-to-adult communication.[2]

Finally, even if Section 223(d)(1)(B) were unconstitutional in some of its applications, the court erred in invalidating both Section 223(d)(1)(A) and Section 223(d)(1)(B) in all their applications. The applicable severability clause, 47 U.S.C. 608, directs courts to preserve all provisions and all applications of the CDA that are constitutional. As we explain in our jurisdictional statement in *ACLU* (at 25-26), under that severability clause, any infirmity in Section 223(d)(1)(B) should not affect Section 223(d)(1)(A). And even if Section 223(d)(1)(B) were unconstitutional in some of its applications, there would be no justification for invalidating Section 223(d)(1)(B) as applied to its other applications.

2. Although the district court's constitutional analysis is seriously flawed, we do not recommend that this Court note probable jurisdiction at this time. The questions at issue in the present appeal are identical to questions raised in the government's appeal in *ACLU*, and the records in the two cases are not materially different. There is therefore no reason for the Court to consider both cases simultaneously.

---

[2] Section 223(d)(2) prohibits any person from "knowingly permit[ting] any telecommunications facility under such person's control to be used for any activity prohibited by" Section 223(d)(1). Because the application of Section 223(d)(2) depends on the application of Section 223(d)(1), its constitutionality does not require separate analysis.

The *ACLU* appeal provides a more appropriate vehicle for addressing the questions that the two cases have in common. The *ACLU* appeal also involves a broader range of issues. That appeal not only raises all the questions presented in this case; it also raises questions concerning the constitutionality of 47 U.S.C. 223(a)(1)(B), which prohibits the use of a "telecommunications device" to knowingly "initiate[] the transmission of any * * * communication which is * * * indecent, knowing that the recipient of the communication is under 18 years of age," and 47 U.S.C. 223(a)(2), which prohibits any person from "knowingly permit[ting] any telecommunications facility under his control to be used for any [such] activity." Those provisions were not challenged by appellee, and the court below therefore did not consider them.

In addition, appellees in the *ACLU* case include a large number of persons and organizations engaged in a wide range of Internet activities, while this case involves a single appellee. Some of the appellees in *ACLU* are electronic journalists, like appellee Shea. Because the present appeal does not raise any question that is not presented in *ACLU*, and the *ACLU* appeal involves a broader range of issues and parties, this Court should hold this case and dispose of it as appropriate in light of its decision in *ACLU*.

CONCLUSION

The appeal in this case should be held pending the Court's decision in *Reno* v. *American Civil Liberties Union*, No. 96-511, and then disposed of as appropriate in light of that decision.

Respectfully submitted.

WALTER DELLINGER
Acting Solicitor General
FRANK W. HUNGER
Assistant Attorney General
EDWIN S. KNEEDLER
Deputy Solicitor General
IRVING L. GORNSTEIN
Assistant to the Solicitor General
BARBARA L. HERWIG
JACOB M. LEWIS
Attorneys

OCTOBER 1996

APPENDIX A

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

No. 96 Civ. 0976 (DLC)

JOE SHEA, ON BEHALF OF THE AMERICAN REPORTER, PLAINTIFF

v.

JANET M. RENO, ATTORNEY GENERAL OF THE UNITED STATES OF AMERICA, DEFENDANT

[Filed: July 29, 1996]

Before: CABRANES, Circuit Judge,* SAND** and COTE,*** District Judges.

The plaintiff, an editor, publisher, and part-owner of a newspaper distributed exclusively through electronic means, brings this First Amendment challenge to § 223(d) of the Communications Decency Act of 1996 ("CDA") criminalizing the use of interactive

---

* The Honorable José A. Cabranes of the United States Court of Appeals for the Second Circuit.

** The Honorable Leonard B. Sand of the United States District Court for the Southern District of New York.

*** The Honorable Denise Cote of the United States District Court for the Southern District of New York.

computer services to display "patently offensive" sexually explicit material such that it is available to persons under the age of eighteen. The plaintiff seeks a preliminary injunction barring application of the section. The three-judge panel, appointed pursuant to 28 U.S.C. § 2284, held that: (1) plaintiff has not sustained his burden of demonstrating a likelihood of success on his claim that § 223(d) is unconstitutionally vague, but that (2) the plaintiff has demonstrated a likelihood of success on his claim that § 223(d) is unconstitutionally overbroad in that it bans protected indecent communication between adults. On this second point, the court concluded that most content providers' ability to comply with the requirements of the affirmative defenses set out in the statute depends on the actions of third parties, such as software manufacturers, whose cooperation is not required under the statute or otherwise mandated. The technological impossibility of independent compliance with the affirmative defenses renders § 223(d) unconstitutional as an overbroad prohibition on constitutionally protected indecent speech between adults.

MEMORANDUM AND ORDER

We address here the constitutionality of a provision of the Communications Decency Act of 1996 ("CDA") with an undeniably worthy goal: to limit the exposure of children to sexually explicit, though not legally obscene, materials available "on line"—that is, capable of being displayed and "accessed" by increasingly common interactive computer services. 47 U.S.C. § 223(d), as added by the CDA on February 8, 1996, criminalizes the use of an interactive computer service to display, in a manner available to persons under eighteen, sexually explicit material that is

"patently offensive" by contemporary community standards. Plaintiff Joe Shea, the editor, publisher, and part-owner of a newspaper distributed solely by electronic means, filed this action on February 8, 1996, claiming that § 223(d) is (1) void for vagueness, in that it fails to give ordinary citizens sufficient notice of what conduct will subject them to prosecution or criminal liability; and (2) substantially overbroad, in that it targets a broader category of speech than necessary to achieve the government's goal and constitutes a ban on certain constitutionally protected speech between adults.

As editor of an on-line newspaper, the plaintiff is one of a growing number of citizens who employ an array of widely accessible and constantly evolving media technologies to gather and disseminate information and ideas. In passing the CDA, Congress explicitly recognized that these technologies foster "true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity." Pub.L. No. 104-104, § 509(a)(3), 110 Stat. 56, 138 (1996) (to be codified at 47 U.S.C. § 230(a)(3)). The range of tools and forums available for users of interactive computer services is astounding: with access to the web of computer networks known as the Internet, a scholar can contact a distant computer and make use of its capabilities; a researcher can peruse the card catalogs of libraries across the globe; users around the world can debate politics, sports, music, and literature. However trivial some of their uses might seem, emerging media technologies quite simply offer an unprecedented number of individual citizens an opportunity to speak and to be heard—at very little cost—by

audiences around the world. In that sense, we are encountering a communications medium unlike any we have ever known.

In an attempt to limit the availability of certain materials in interactive computer services, Congress enacted a statute of unprecedented sweep: the new § 223(d) purports to regulate not only how commercial purveyors of obscene or pornographic materials may advertise and sell their products on line, but also how private individuals who choose to exchange certain constitutionally protected communications with one another can do so. The question presented is whether our Constitution tolerates this level of governmental intrusion into how adults speak to one another.

We conclude, first, that the plaintiff has not sustained his burden of demonstrating a likelihood of success on his claim that § 223(d) is unconstitutionally vague. The definition of material regulated by this section is a familiar one, repeatedly upheld against vagueness challenges in a line of jurisprudence concerning television and radio broadcasting, cable programming, and commercial telephone services. We do, however, conclude that the plaintiff has demonstrated a likelihood of success on his overbreadth claim, that § 223(d) would serve as a ban on constitutionally protected indecent communication between adults. The Government concedes that strict scrutiny is appropriately applied to this claim and that § 223(d) would, on its own, act as an unconstitutional total ban on indecent communication, protected and unprotected alike, but argues that two affirmative defenses set out in § 223(e)(5) serve to shield adults engaging in constitutionally protected indecent communication from criminal liability.

The evidentiary record in this case compels the conclusion that, given the current state of technology, most adult content providers wishing to engage in constitutionally protected indecent speech will be unable to avail themselves of these affirmative defenses. Only a limited subset of on-line content providers, commercial providers on the World Wide Web, can avail themselves of the defense set out in § 223(e)(5)(B), leaving both non-commercial providers of Web content and content providers using all other modes of on-line communication unprotected. The evidence further demonstrates that content providers' ability to comply with the terms of the second defense—the so-called good-faith defense—depends on the actions of third parties, such as software manufacturers, whose cooperation is not required under the CDA or otherwise mandated. There is no feasible means, with our current technology, for someone to provide indecent content on line with any certainty that even his best efforts at shielding the material from minors will be "effective," as the language of the good-faith defense requires.

Because neither of the affirmative defenses set out in § 223(e)(5) can, with our current technology, effectively protect adult content providers wishing to engage in constitutionally protected indecent communication, we reach the inescapable conclusion that § 223(d) will serve to chill protected speech. We therefore find that the plaintiff has demonstrated a likelihood of success on the merits of his claim that § 223(d) is unconstitutionally overbroad.

We are mindful of our obligation to construe a federal statute to avoid constitutional problems if it is

possible to do so, but we are equally mindful of the limits of the judicial power under our Constitution and we decline the Government's invitation to perform radical surgery on a statute dealing with a difficult problem in a rapidly changing area of technology; in sum, we respectfully decline the invitation to legislate from the bench.

In setting aside the challenged provisions, we do not question the legitimacy of the government's interest in safeguarding children from exposure to certain materials available on line nor suggest that other legislation on another day, carefully tailored to technological realities, may not pass constitutional muster. We also do not consider, nor attempt to delineate, the range of circumstances, if any, in which Congress could now or in the future constitutionally impose content-based restrictions upon communications in the developing medium we explore here.

I. BACKGROUND

Plaintiff Joe Shea is the editor-in-chief, part-owner, and publisher of the *American Reporter*, a daily newspaper distributed solely by electronic means. On February 8, 1996, following the signing of the Telecommunications Act of 1996, Pub.L. No. 104-104, 110 Stat. 56, the *American Reporter* published an editorial, (Complaint, Ex. 1) criticizing Title V of the Act, known as the Communications Decency Act of 1996 ("CDA"). The editorial contained language arguably falling within the scope of a provision of the CDA criminalizing the transmission or display of certain content in a manner available to minors:

Whoever—

(1) in interstate or foreign communications knowingly—

(A) uses an interactive computer service to send to a specific person or persons under 18 years of age, or

(B) uses any interactive computer service to display in a manner available to a person under 18 years of age, any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs, regardless of whether the user of such service placed the call or initiated the communication; . . .

shall be fined under title 18, United States Code, or imprisoned not more than two years, or both.

Pub.L. No. 104-104, § 502(2)(d), 110 Stat. at 133 (to be codified at 47 U.S.C. § 223(d)). Also on February 8, the plaintiff filed this action on behalf of the *American Reporter*, seeking a declaration that 47 U.S.C. § 223(d) is unconstitutionally overbroad and vague. On February 17, the plaintiff moved for preliminary injunctive relief to prevent the Department of Justice from enforcing the provision in question.

Pursuant to § 561(c) of the Telecommunications Act and 28 U.S.C. § 2284, the Chief Judge of the United States Court of Appeals for the Second Circuit designated this three-judge district court to consider the plaintiff's facial challenge to the constitutionality of § 223(d). The Court heard opening

arguments on April 3, 1996. Because the plaintiff's facial challenge to § 223(d) raised the question of whether Internet users can, under current technology, meet the requirements for certain defenses provided for in the Act, the Court concluded that an evidentiary hearing would be appropriate. In light of the pendency of consolidated proceedings for preliminary injunctive relief before a three-judge court in the Eastern District of Pennsylvania raising, among other claims, a facial challenge to § 223(d), *see* Complaint, *American Civil Liberties Union v. Reno*, No. 96-963 (E.D.Pa. filed Feb. 8, 1996); Complaint, *American Library Ass'n v. U.S. Dep't of Justice*, No. 96-1458 (E.D.Pa. filed Feb. 27, 1996) (collectively "the Philadelphia litigation"), the Court directed the parties to consider methods of easing the fact-finding process by entering into a range of stipulations regarding the current state of technology and incorporating relevant portions of the record in the Philadelphia litigation. The Court received additional demonstrative and testimonial evidence on April 29, April 30, and May 6, and heard closing arguments on June 3, 1996. Following supplemental briefing by the parties, the plaintiff's motion for preliminary injunctive relief was submitted for decision on June 13, 1996.

On June 11, 1996, the three-judge court in the Philadelphia litigation concluded, *inter alia*, that the provision of the CDA here challenged by the plaintiff does not withstand constitutional scrutiny. *American Civil Liberties Union v. Reno*, 929 F.Supp. 824, 849 (E.D.Pa.1996) ("*ACLU/ALA*"). All three judges agreed that the CDA is substantially overbroad, in that it effectively forces many Internet users (specifically, non-commercial, not-for-profit entities and

"even many commercial organizations") to forgo constitutionally protected speech or risk criminal prosecution. *Id.* at 853-855 (Sloviter, C.J.); *id.* at 857 (Buckwalter, J.); *id.* at 869 (Dalzell, J.). Additionally, two of the judges concluded that § 223(d)'s definition of covered speech is unconstitutionally vague. *Id.* at 856 (Sloviter, C.J.); *id.* at 857 (Buckwalter, J.). The decision in the Philadelphia litigation does not preclude this Court from deciding the issues presented,[1] to which we now turn.

---

[1] Following the Philadelphia decision, the Court ordered the parties to file letter briefs addressing the preclusive effect, if any, of the Philadelphia court's findings of fact on this proceeding. "Under the judicially developed doctrine of collateral estoppel, once a court has decided an issue of fact or law necessary to its judgment, that decision is conclusive in a subsequent suit based on a different cause of action involving a party to the prior litigation." *United States v. Mendoza*, 464 U.S. 154, 158, 104 S.Ct. 568, 571, 78 L.Ed.2d 379 (1984). Although the doctrine can apply where there is no mutuality of parties and can be used offensively, *id.* at 158-59, 104 S.Ct. at 571-72, *Mendoza* makes clear that nonmutual offensive collateral estoppel does not apply against the government, at least as to issues of law, *id.* at 162-63, 104 S.Ct. at 573-74. Although courts have observed that *Mendoza* leaves open the possibility that nonmutual collateral estoppel may apply against the government with respect to factual issues, *see, e.g., Adkins v. Commissioner of Internal Revenue*, 875 F.2d 137, 141 (7th Cir.1989), we conclude that its application is inappropriate here in light of the "avowedly tentative" nature of the Philadelphia court's findings. *Lummus Co. v. Commonwealth Oil Refining Co.*, 297 F.2d 80, 89 (2d Cir.1961), *cert. denied*, 368 U.S. 986, 82 S.Ct. 601, 7 L.Ed.2d 524 (1962); *see ACLU/ALA*, 929 F.Supp. at 838 ("Because of the rapidity of developments in this field, some of the technological facts we have found may become partially obsolete by the time of publication of these [f]indings."). Although many of our findings overlap with those made in *ACLU/ALA*, we recognize that Internet technology is rapidly

II. FINDINGS OF FACT

We enter the following findings of fact, many of which are undisputed, the subject of stipulations by the parties, or submitted by the defendant and adopted by us, pursuant to Rule 52(a) of the Federal Rules of Civil Procedure. Although we here consider a so-called facial challenge to a statute, we deemed it appropriate and necessary in the unusual circumstances presented here, and a reasonable exercise of our discretion, to establish a basic record of the facts regarding the new and evolving communications media that is the subject of this legislation.

Section 223(d) targets the use of an "interactive computer service" to send or display patently offensive materials. Although § 223 itself contains no definition of that term, the definition applicable to the new 47 U.S.C. § 230—also added by the CDA—makes clear that the term encompasses means of making "content"[2] available to multiple users both on the vast web of linked networks popularly known as "the Internet" and on other information systems (such as electronic bulletin boards maintained by educational institutions or nonprofit organizations) not physically linked to the Internet. *See* Pub.L. No. 104-104, § 509(e)(2), 110 Stat. at 139 (to be codified at 47 U.S.C. § 230(e)(2)). We draw upon the stipulations of the parties and the testimony adduced at the three-day

---

evolving, and that evidence of new developments was added to the record before us as late as June 7, 1996.

[2] We use the term "content" to refer to any text, data, sound, program, or visual image transmitted over or made available for retrieval on an interactive computer service.

evidentiary hearing to describe: (1) the nature of the medium targeted by § 223(d), focusing in part on the degree of control that those who transmit content have over who will receive it; (2) the availability of certain categories of potentially objectionable material on line; (3) the development of software and labeling standards enabling parents to limit their children's exposure to objectionable on-line content; and (4) the potential for tagging and verification procedures that content providers can use in an effort to shield minors from sexually explicit content that they provide.[3] As we do so, we unavoidably—and with apologies to all others with a similar aversion to "cyberspeak"—adopt some of the terminology that has developed in conjunction with this technology. We endeavor, to the extent possible, to avoid the jargon of this field, and to define our terms wherever possible, for the sake of the clarity of this record and this opinion, as well as for the benefit of any reader required to review our work.

A. *The Development of the Internet*

Although "the Internet" now formally describes a collection of more than 50,000 networks linking some nine million host computers in ninety countries, it has existed for nearly three decades on a much smaller scale. What we now refer to as the Internet grew out of an experimental project of the Department of Defense's Advanced Research Projects Ad-

---

[3] While § 223(d) regulates more than the content of Internet communications, we focus mainly on the range of tools and services available to individuals with Internet access, recognizing that the vast majority of content available through the use of an interactive computer service is in fact available on the Internet.

ministration ("ARPA") designed to provide researchers with direct access to supercomputers at a few key laboratories and to facilitate the reliable transmission of vital communications. (Declaration of William J. Hoffman ("Hoffman Decl."), Ex. 4, at 11-12) ARPA supplied funds to link computers operated by the military, defense contractors, and universities conducting defense-related research through dedicated phone lines, creating a "network" known as ARPANet. (Parties' Stipulations in Preparation for Preliminary Injunction Hearing ("Joint Stip.") ¶¶ 6-7; Hoffman Decl., Ex. 3, at 3; *id.* Ex. 4, at 11) Programs on the linked computers implemented a technical scheme known as "packet- switching," through which a message from one computer to another would be subdivided into smaller, separately addressed pieces of data, known as "packets," sent independently to the message's destination and reassembled upon arrival. (Joint Stip. ¶ 9) Each computer on the network was in turn linked to several other computers, creating any number of routes that a communication from one computer could follow to reach its destination. If part of the network were damaged, a portion of the message could be re-routed automatically over any other path to its ultimate destination, a characteristic of the network intended initially to preserve its operability in the event of enemy attack. (*Id.* ¶¶ 7-8; Hoffman Decl., Ex. 3, at 3; *id.* Ex. 4, at 12)

Having successfully implemented a system for the reliable transfer of information over a computer network, ARPA began to support the development of communications protocols for transferring data between different types of computer networks. Univer-

sities, research facilities, and commercial entities began to develop and link together their own networks implementing these protocols; these networks included a high-speed "backbone" network known as NSFNet, sponsored by the National Science Foundation, smaller regional networks, and, eventually, large commercial networks run by organizations such as Sprint, IBM, and Performance Systems International (commonly known as "PSI"). (Hoffman Decl., Ex. 3, at 3; *id.* Ex. 4, at 13-14) As faster networks developed, most network traffic shifted away from ARPANet, which formally ceased operations in 1990. (*Id.* Ex. 3, at 3) What we know as "the Internet" today is the series of linked, overlapping networks that gradually supplanted ARPANet. Because the Internet links together independent networks that merely use the same data transfer protocols, it cannot be said that any single entity or group of entities controls, or can control, the content made publicly available on the Internet or limits, or can limit, the ability of others to access public content. Rather, the resources available to one with Internet access are located on individual computers around the world. (Joint Stip. ¶ 11)

It is estimated that as many as forty million individuals have access to the information and tools of the Internet, and that figure is expected to grow to 200 million by the year 1999. (*Id.* ¶ 3) Access to the Internet can take any one of several forms. First, many educational institutions, businesses, libraries, and individual communities maintain a computer network linked directly to the Internet and issue account numbers and passwords enabling users to

gain access to the network directly or by modem.[4] (*Id.* ¶¶ 12-14) Second, "Internet service providers," generally commercial entities charging a monthly fee, offer modem access to computers or networks linked directly to the Internet. (*Id.* ¶ 16) Third, national commercial "on-line services"—such as America Online, CompuServe, Prodigy, and Microsoft Network—allow subscribers to gain access to the Internet while providing extensive content within their own proprietary networks. (*Id.* ¶ 17) Finally, organizations and businesses can offer access to electronic bulletin-board systems—which, like national on-line services, provide certain proprietary content; some bulletin-board systems in turn offer users links to the Internet. (*Id.* ¶ 18)

B. *Categories of Internet Use*

For our purposes, there are two loose and overlapping categories of Internet use. First, an individual who has secured access to the Internet can correspond or exchange views with one or many other Internet users. Second, a user can locate and retrieve information available on other computers. We explore these categories in greater detail below. As will become clear, distinctions in how Internet content is transmitted affect the degree of control that providers of content have over who will be able to gain access to their communications;[5] we will return to

---

[4] A "modem" (a contraction of "modulator" and "demodulator") is a device that translates digital information into a signal for transmission over a telephone line ("modulation") and translates a signal received over a telephone line into digital information ("demodulation").

[5] We use the term "content provider" to refer to any Internet "speaker"—that is, a user who transmits or makes

the legal significance of these distinctions at a later juncture. For any communication to take place over the Internet, two pieces of software,[6] adhering to the same communications protocol, are required. A user must have access to certain kinds of "client" software, which enables his computer to communicate with and make requests of remote computers where information is stored; these remote computers must be running "server" software, which provides information in response to requests by client software. (Declaration of Dr. Dan R. Olsen, Jr. ("Olsen Decl."), ¶¶ 13-14)[7]

1. *Communicating with Other Internet Users*

Perhaps the most widely used Internet service is electronic mail, or "e-mail." Using any one of dozens of available "mailers"—client software capable of

---

available any content over the Internet. Although the term is not used in the statutory provision at issue, "information content provider" is elsewhere defined in the CDA as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." Pub.L. No. 104-104, § 509(e)(3), 110 Stat. at 139 (to be codified at 47 U.S.C. § 230(e)(3)). The phrase serves as a reasonable shorthand for the category of individuals targeted by the CDA—persons who send or display Internet content. *See* S. CONF. REP. NO. 230, 104th Cong., 2d Sess. 188 (1996) (stating that § 223(d)(1) applies to "content providers").

[6] We use the term "software" to refer to the combination of programs and procedures that serve as instructions to the computer. The term is often used in contrast with "hardware," which refers to a computer system's physical elements.

[7] The Court received direct testimony of the parties' experts on technological issues (Dr. Olsen for the defendants and Clay Shirky for the plaintiffs) by affidavit.

reading and writing e-mail—a user is able to address and transmit a message to one or more specific individuals. (Joint Stip. ¶ 21) A user can also "subscribe" to an electronic mailing list on a topic of interest; the user receives a copy of messages posted by other subscribers and, in turn, can post messages for forwarding to the full mailing list. Once a mailing list is established, it is typically maintained using a "mail exploder"—a program such as "listserv" running on the server on which the list resides—that automatically (*i.e.*, without human intervention) responds to a user's request to be added to or removed from the list of subscribers and retransmits messages posted by a subscriber to others on the mailing list. (*Id.* ¶ 22) Some mailing lists are "closed": a user's request to join the list requires the approval of an individual who maintains the list. (*Id.*) Mailing lists (both open and closed) may also be "moderated": all messages posted to the list are forwarded to a moderator, who approves certain messages and retransmits them to subscribers. (*Id.*) An individual sending a message that will be retransmitted by a mail exploder program has no way of knowing the e-mail addresses of other subscribers. (Olsen Decl. ¶ 19; Testimony of Gordon C. Galligher, Jr., Tr. at 181) Even if the user could obtain an e-mail address for each subscriber to a particular list, those addresses alone would provide no authoritative information about subscribers. There is no directory that identifies persons using a certain e-mail address. In addition, a user can avoid disclosing his true e-mail address by developing an e-mail "alias" or by using an "anonymous remailer"—a server that purges identifying information from a communication before forwarding it to its destination. (Defendant's Response

to Plaintiff's Request for Admissions ("Defendant's Adm.") No. 22; Galligher Test., Tr. at 173)

Internet users may also transmit or receive "articles" posted daily to thousands of discussion groups, arranged by subject matter and known as "newsgroups," available through an electronic bulletin-board system known as "Usenet." When a user with access to a Usenet server—that is, a computer participating in the Usenet system—posts an article to a particular newsgroup, the server automatically forwards the article to adjacent Usenet servers, which in turn forward it to other servers, until the article is available on all Usenet sites that furnish access to the newsgroup in question. (Joint Stip. ¶ 23) Once a message reaches a particular Usenet site, it is temporarily stored there so that individual users—running client software, known as a "newsreader," capable of sorting articles according to header information identifying the newsgroup to which the article was posted—can review and respond to the message. (*Id.*; Hoffman Decl., Ex. 4, at 129) Some Usenet newsgroups are moderated; messages to the newsgroup are forwarded to an individual who selects those appropriate for distribution. (Joint Stip. ¶ 23) Because Usenet articles are distributed to (and made available on) multiple servers, one who posts an article to a newsgroup has no way of knowing who will choose to retrieve it, whether or not the newsgroup is moderated. (Galligher Test., Tr. at 170, 174-75) There is no newsgroup equivalent of a "closed" mailing list: access to a particular newsgroup can only be limited by restricting the number of servers participating in the newsgroup. (Testimony of Clay Shirky, Tr. at 251)

The Internet also offers opportunities for multiple users to interact in real time. Using a program called "Talk," two users can exchange messages while they are both on line; a message typed on one user's computer will appear almost immediately on the other's screen. (Joint Stip. ¶ 25) Servers running so-called "chat" software, such as Internet Relay Chat ("IRC"), permit multiple users to converse by selecting one of many discussion "channels" active at any time. Commercial on-line services such as America Online, CompuServe, Prodigy, and the Microsoft Network offer their own chat systems for their members. (*Id.* ¶ 26) Having joined a channel, the user can see and read messages transmitted by other users, each identified by a name the user selects upon joining the channel. (*Id.* ¶ 25) Individual participants in IRC discussions know other participants only by the names they choose upon entering the discussion; users can participate anonymously by using a pseudonym.

2. *Locating and Retrieving Information on the Internet*

Individuals with Internet access can take advantage of a number of tools for locating and retrieving information and resources stored on remote computers. One who wishes to make certain articles, files, or software available to other users will set up a server, adhering to certain communications protocols, capable of retrieving and presenting stored information in response to a request from client software using the same communications protocol. (Olsen Decl. ¶¶ 13, 16; Galligher Test., Tr. at 131)

a. *File-Transfer Protocol ("FTP")*

One type of software implements a set of conventions for copying files from a host computer known as "file-transfer protocol" ("FTP"). With appropriate client software, a user with an account on the host computer can contact the server, view a directory of available files, and copy one or more of those files to his own computer. In addition to making files available to users with accounts, thousands of content providers also make files available for "anonymous" retrieval by users who do not possess an account on the host computer.[8] (Hoffman Decl., Ex. 3, at 1-2, 5; *id.* Ex. 4, at 187; Joint Stip. ¶ 29) A content provider who makes files available for retrieval by anonymous FTP has no way of discerning who gains access to the files.

b. *"Gopher" Servers*

A second type of server software capable of making available the resources of a host computer is known as a "gopher" program. (Joint Stip. ¶ 30, Hoffman Decl., Ex. 3, at 5) A gopher server presents information in a set of menus, enabling a user who gains access to the server to select a series of increasingly narrow menu items before locating a desired file that can be displayed on or copied to the user's computer.[9]

---

[8] To locate files available for copying, a user can contact an "Archie" server—a remote computer capable of searching directories for file names containing a particular string of characters on FTP servers permitting anonymous retrieval. (Hoffman Decl., Ex. 4, at 180-90)

[9] As with FTP servers, there are tools available for locating menus or items containing a certain string of characters: a "Veronica" server is capable of searching menus on all gopher servers, while "Jughead" is an aptly named tool for

(Galligher Test., Tr. at 122; Hoffman Decl., Ex. 3, at 5) A content provider who maintains a gopher server ordinarily has no way of knowing who will gain access to the information made available.

c. *The World Wide Web*

The third and perhaps best known method of locating and accessing information on the Internet is by exploring the World Wide Web. Documents available on the Web are not collected in any central location; rather, they are stored on servers around the world running Web server software. (Joint Stip. ¶¶ 31, 38, 40) To gain access to the content available on the Web, a user must have a Web "browser"—client software, such as Netscape Navigator, Mosaic, or Internet Explorer, capable of displaying documents formatted in "hypertext markup language" ("HTML"), the standard Web formatting language. (Galligher Test., Tr. at 125; Joint Stip. ¶¶ 31, 43) Each document has an address, known as a Uniform Resource Locator ("URL"), identifying, among other things, the server on which it resides; most documents also contain "links"—highlighted text or images that, when selected by the user, permit him to view another, related Web document. (Joint Stip. ¶ 34) Because Web servers are linked to the Internet through a common communications protocol, known as hypertext transfer protocol ("HTTP"), a user can move seamlessly between documents, regardless of their location; when a user viewing a document located on one server selects a link to a document located elsewhere, the browser will automatically

---

searching menus on only a single server. (Galligher Test., Tr. at 124; Hoffman Decl., Ex. 3, at 5; *id.* Ex. 4, at 191-92)

contact the second server and display the document. (Joint Stip. ¶¶ 34, 37) Some types of Web client software also permit users to gain access to resources available on FTP and gopher sites.

A number of "search engines"—such as Yahoo, Magellan, Alta Vista, WebCrawler, and Lycos—are available to help users navigate the World Wide Web.[10] For example, the service Yahoo maintains a directory of documents available on various Web servers. A user can gain access to Yahoo's server and type a string of characters as a search request. Yahoo returns a list of documents whose entries in the Yahoo directory match the search string and organizes the list of documents by category. (Galligher Test., Tr. at 134; Plaintiff's Ex. 3) Search engines make use of software capable of automatically contacting various Web sites and extracting relevant information. Some search engines, such as Alta Vista, store the information in a database and return it in response to a user request. Others, such as Yahoo, employ a group of individuals to determine whether and how a site should be categorized in the Yahoo directory. (Galligher Test., Tr. at 137; Supplemental Declaration of William J. Hoffman ("Hoffman Supp.Decl.") Ex. A, at 39-42 (Testimony of Donna L. Hoffman in *ACLU/ALA*))

As the growth in Internet use and the wide availability of tools and resources to those with access to the Internet suggest, the Internet presents extremely low entry barriers to those who wish to

---

[10] Most of these services do not charge users for search requests and are sustained primarily by advertising revenues. (Galligher Test., Tr. at 136-37)

convey Internet content or gain access to it. In particular, a user wishing to communicate through e-mail, newsgroups, or Internet Relay Chat need only have access to a computer with appropriate software and a connection to the Internet, usually available for a low monthly fee. The user then in a sense becomes a public "speaker," able to convey content, at relatively low cost, to users around the world to whom it may be of interest. Those who possess more sophisticated equipment and greater technical expertise can make content available on the Internet for retrieval by others (known or unknown) by running a server supporting anonymous FTP, a gopher server, or a Web server. Yet content providers need not necessarily run their own servers or have the programming expertise to construct their own sites; they can lease space on a Web server from another or create a "home page" through an on-line commercial service.

The ease of entry of many speakers sets interactive computer systems apart from any other more traditional communications medium that Congress has attempted to regulate in the past. With one-way media such as radio and television broadcasting or cable programming, a user is merely a listener or viewer; in the CDA, Congress sought to target "interactive" computer systems through which a listener or viewer, by definition, has the power to become a speaker. The relative ease of speaker entry and the relative parity among speakers accounts for the unprecedented and virtually unlimited opportunities for political discourse, cultural development, and intellectual activity that Congress found to characterize emerging communication technologies.

In seeking to describe the range of tools and opportunities for Internet users to "speak," we recognize that the categories we delineate are far from clean and the technology is far from static. Indeed, by all indications, the way that we conceptualize various media that we have traditionally viewed as distinct—such as cable television, telephones, and computer networks—will change dramatically as these media "converge" into common forms of communication. *See Denver Area Educ. Telecommunications Consortium v. FCC* ("*Denver Area Consortium*"), — U.S. ——, —— & n. 4, 116 S.Ct. 2374, 2402 & n. 4, — L.Ed.2d —— (1996) (Souter, J., concurring); *see also* Jerry Berman & Daniel J. Weitzner, *Abundance and User Control: Renewing the Democratic Heart of the First Amendment in the Age of Interactive Media*, 104 YALE L.J. 1619, 1619 n. 1 (1995); Art Kramer, *Netwatch: The AJC's Daily Online Guide*, ATL.J. & CONST., May 29, 1996, at B04 (describing cable modem technology designed to offer Internet access through existing cable television connections) (Hoffman Supp.Decl., Ex. C, at 3-4). Of course, our findings of fact are necessarily time-bound. We can only determine whether the statutory provision at issue here, in light of the technology available during the pendency of this case, comports with the First Amendment.

C. *Sexually Explicit Content on the Internet*

It is undisputed that there exists some content on the Internet that is—to use the Government's phrase—"sexually explicit." (Defendant's Memorandum of Law, filed March 19, 1996, at 11) The term "sexually explicit" is descriptive rather than legal and does not appear in the statutory provision at

issue, but the Government employs it as a shorthand to describe Internet content depicting "sexual or excretory activities or organs"—possibly though not necessarily in a patently offensive way. (Defendant's Supplemental Memorandum of Law ("Defendant's Supp. Memo."), filed June 7, 1996, at 9) That is, the Government does not contend that all sexually explicit material is "patently offensive" and therefore within the scope of the CDA, but claims that there is certainly content available on the Internet that is both sexually explicit and patently offensive.

The testimony and demonstration of one of the Government's expert witnesses, Howard Schmidt, Director of the Air Force Office of Special Investigations, amply confirmed the availability of sexually explicit material on line. Nevertheless, there is no persuasive evidence in the record to suggest, much less prove, that sexually explicit material easily "assaults" an unknowing user—as in other media, most notably television and radio—or that any substantial proportion of Internet content is sexually explicit.

1. *Ease of Access to Sexually Explicit Content*

The Government urges us to conclude that an Internet user can easily stumble upon sexually explicit material. (Defendant's Post-Hearing Memorandum of Law ("Defendant's Post-Hearing Memo."), filed May 28, 1996, at 31-32) It is important to begin with the general observation that, with the exception of e-mail, no content appears on a user's screen without the user having first taken some affirmative step. One wishing to read articles posted to a newsgroup must connect to a Usenet server and select the

relevant group. To retrieve a file through anonymous FTP or access a gopher server, the user must search for or know the address of a particular server. To gain access to content on the World Wide Web, a user must know the URL of a relevant site or type a keyword into one of several available search engines.

Schmidt's demonstration focused mainly on the availability of sexually explicit content on the World Wide Web. In the absence of any screening software or filter, a user determined to view a site containing sexually explicit material can certainly do so, either by typing a known URL or by searching for key words. One sexually explicit site may, in turn, contain "links" to other such sites. (Defendant's Exs. 13, 16, 17, 26, 29, 32; Schmidt Test., Tr. at 401-02) While ordinarily a user must affirmatively seek sexually explicit material to view it, on occasion a search not intended to retrieve sexually explicit material may retrieve a link to a sexually explicit site. For example, Schmidt's searches of "Sleeping Beauty," "Babe," and "Little Women" produced a handful of links to sexually explicit sites. (Defendant's Exs. 15, 18, 27, 31, 38) This demonstration revealed the inevitable imprecision of search engines—a broad search will almost always return some irrelevant results. In the vast majority of cases, the character of a sexually explicit site will be clear from the entry or link that a search engine returns. Nevertheless, there is potential for occasional accidental viewing of sexually explicit material. For example, if a user were to view entries in a WebCrawler search using that program's standard format as preset by the manufacturer, he would see no summary of the sites' contents. (Defendant's Ex. 18; Shirky Test., Tr. at

237-38) One of Schmidt's searches of "Sleeping Beauty" returned an entry offering a link to a site containing sexually explicit material; the entry (when viewed apart from other entries on the same page with similar addresses) gave little indication of the site's contents. (Defendant's Ex. 15; Shirky Test., Tr. at 238) It is difficult to know how often accidental viewing can occur, but there is no basis in the record for concluding that a user not seeking out sexually explicit material on the Internet will encounter it with any particular frequency.

2. *The Availability of Sexually Explicit Content*

Although Schmidt's demonstration focused on the World Wide Web, sexually explicit content is available on the Internet through almost any form of Internet communication. Yet there is no evidence that sexually explicit content constitutes a substantial—or even significant—portion of available Internet content. While it is difficult to ascertain with any certainty how many sexually explicit sites are accessible through the Internet, the president of a manufacturer of software designed to block access to sites containing sexually explicit material testified in the Philadelphia litigation that there are approximately 5,000 to 8,000 such sites, with the higher estimate reflecting the inclusion of multiple pages (each with a unique URL) attached to a single site. (Stipulated Portions of Record in *ACLU/ALA* ("Stipulated Record"), Ex. M, at 139-40 (Testimony of Ann W. Duvall in *ACLU/ALA*)) The record also suggests that there are at least thirty-seven million unique URLs. (Galligher Test., Tr. at 144) Accordingly, even if there were twice as many unique pages on the Internet containing sexually explicit materials

as this undisputed testimony suggests, the percentage of Internet addresses providing sexually explicit content would be well less than one tenth of one percent of such addresses.

It is not disputed that some of the sexually explicit materials that the CDA attempts to keep away from minors originates abroad. This is not surprising inasmuch as forty percent of all host computers are located outside the United States. (Joint Stip. ¶ 3) Although only a tentative approximation is possible, the record suggests that as much as thirty percent of the sexually explicit material currently available on the Internet originates in foreign countries. (Stipulated Record, Ex. L, ¶ 41; *id.* Ex. M, at 161-62 (Duvall Test.))

D. *The Development of Blocking Tools and Labeling Schemes*

As the Internet has become accessible to more households, several commercial on-line services and software companies have developed features and packages designed to enable parents to limit children's exposure to potentially inappropriate Internet material. For example, America Online, Prodigy, and Microsoft Network, which permit their subscribers to obtain access to Internet material, offer parental control options free of charge to their members. (Joint Stip. ¶ 67) America Online, for example, allows parents to establish a separate account for their children limited to the service's own proprietary content. (*Id.*) In addition, at least one type of screening software, SurfWatch, has a feature allowing parents to block access to all Internet sites except for those that parents choose to make available to their

children. (Stipulated Record, Ex. M, at 131 (Duvall Test.))

The Government offered testimony and a demonstration regarding SurfWatch (configured to act as a screening tool, rather than to block all Internet access) and a second type of screening software, Cyber Patrol. SurfWatch and Cyber Patrol maintain lists of sites known to contain sexually explicit material; when operating while a user attempts to retrieve Internet material, access to sites identified on their programs will be blocked. In addition, the programs block access to sites whose URLs contain particular character patterns or words, such as "xxx" or "sex," and block any searches including those character patterns or words.

Because of the constant change in the number and location of Internet sites, both SurfWatch and Cyber Patrol offer regular subscription or update services. But even where a parent has properly installed screening software and the software is operational (and configured to block access to certain sites rather than to the entire Internet), it is possible to retrieve some sexually explicit material. The Government's witness was able to run searches using "Babe" and "Little Women" as key words with screening software running in the background. As with searches performed in the absence of screening software, the searches returned links to sexually explicit materials. Some of the links were not blocked by the screening tool. In addition, the Government's witness obtained access to sexually explicit material by directly entering URLs obtained from earlier searches conducted without blocking software in the background. The record also shows that blocking

software is not widely owned by or used in households with access to the Internet: nearly seventy percent of SurfWatch's 1,500 subscribers are schools rather than individual households. (*Id.* at 163-65)

Other efforts to assist parents in filtering and screening material that their children can view on the Internet are under way. The World Wide Web Consortium ("W^{3}C") has launched the Platform for Internet Content Selection ("PICS") to develop technical standards for attaching electronic ratings to Internet addresses. (Joint Stip. ¶¶ 47-49; Stipulated Record, Ex. J., at 1; *id.* Ex. G, at 2-3 (Declaration of Albert Vezza in *ACLU/ALA*)) When the system is fully implemented, PICS-compatible client software (including browsers, newsgroup readers, and mail readers); Internet service providers; and commercial on-line services will be able to detect PICS tags and block content based on how a parent has configured the software. (Joint Stip. ¶ 48; Stipulated Record, Ex. G., at 3 (Vezza Decl.)) PICS will thus enable parents to design from an array of categories blocking criteria that suit the parents' values or needs. The PICS program envisages both rating by content providers and rating by third parties. (Joint Stip. ¶ 48) The vast majority of Internet sites currently remain unrated. Nevertheless, Microsystems Software, Inc. (which manufactures Cyber Patrol) introduced a PICS ratings server in February 1996. (*Id.* ¶ 54) Cyber Patrol is itself now PICS-compatible; it can screen out material based on its PICS tag. (*Id.*) In addition, Microsoft released the first PICS-compatible Web browser, Internet Explorer 3.0, on May 28, 1996. The browser allows parents to block children's access to all unrated Internet sites and to

specify appropriate levels of violence or nudity at rated sites. (Hoffman Supp.Decl., Ex. C, at 1-3)

In addition to PICS tags, the Government's expert witness, Dr. Dan Olsen, testified that content providers wishing to transmit or make available material potentially falling within the scope of the CDA could develop a general practice of inserting a "tag" or "label"—a string of characters, such as "-L18" (for "not less than 18 years")—into the address or name of a particular site so as to clearly identify the site as unsuitable for minors. To transmit or gain access to Internet content, a user must specify a textual name: one cannot send e-mail without an e-mail address or the name of a mailing list; post an article to a newsgroup without specifying the name of the group; participate in the Internet Relay Chat without specifying a "channel"; or access a file without its address. (Olsen Decl. ¶¶ 22-26) Accordingly, content providers using all significant modes of Internet communication could use a tag to identify their content as "covered" content. For example, when a sender transmits an e-mail message, the message is accompanied by the sender's address, which contains a "user name" identifying a particular user and a "domain name" assigned to a computer or set of computers.[11] (Olsen Decl. ¶¶ 25, 60) If the string -L18 were added to the domain name, all e-mail originating from that site—regardless of the particular user who transmitted it—would be identified as containing material falling within the scope of

---

[11] In the example jdoe@smith.com, "smith.com" would constitute a domain name.

the CDA.[12] In the alternative, a particular user name—rather than a domain name—could contain the "-L18" tag; only e-mail originating under that user name would be tagged.[13] Finally, a tag could be placed in a textual subject line, so as to identify only particular messages (rather than all e-mail sent under a certain user name or from a certain computer) as containing content potentially within the scope of the CDA. (*Id.* ¶¶ 60-62)

Similarly, a tag such as "-L18" could be added to the name of a newsgroup; an individual user wishing to post an article potentially falling within the scope of the CDA to a newsgroup that does not as a general matter contain such material could insert a tag in the subject line accompanying the article. (*Id.* ¶¶ 64-65) A tag could also be placed in the name of an IRC channel.

Turning to means of making files available for retrieval or viewing by remote users—using an FTP, gopher, or Web server—content providers could insert a specific tag such as "-L18" in a domain name or site name. Thus, as the Government's expert witness testified, an owner of a Web site named "www.cyberporn.com" could rename the site "www-L18.cyberporn.com". (*Id.* ¶ 51) If a site only contained specific files falling within the scope of the CDA, a content provider could identify those files by adding a tag to the name of the directory in which the file resides or to the file name itself. That is, a file

---

[12] Following the example above, all e-mail would originate from the domain smith-L18.com.

[13] In the example above, material would originate from the address jdoe-L18@smith.com.

identified with the address "http://www.adult.com/picture1.html/" could be renamed "http://www. adult. com/picture1-L18.html/"; in the alternative, a content provider could place all covered files within a specific directory, such as "http://www.adult.com/pictures-L18/". (*Id.* ¶¶ 51-54) A content provider who did not wish to tag an entire file available on a Web server as unsuitable for minors could place a tag within the HTML source code of the file, thus identifying a particular section as subject to the CDA. (*Id.* ¶ 58) In any of these approaches, tagging content is, in a technical sense, a trivial act. (*Id.* ¶¶ 59, 62; Stipulated Record, Ex. B, at 56 (Testimony of Scott O. Bradner in *ACLU/ALA*))

There is an alternative means to shield minors from sexually explicit content available uniquely to content providers on the World Wide Web: verification of a user's "adulthood" before allowing him access to a site. A content provider operating a Web server can create and display an electronic form to retrieve information from a user visiting the Web site; after processing the information by using a program such as a Common Gateway Interface ("cgi") script, the server could grant or deny access to the site. (Shirky Decl. ¶ 21) Not all content providers who make material available on the Web, however, can use programs such as cgi scripts; for example, commercial on-line services such as America Online and CompuServe provide subscribers with the opportunity to post content by configuring their own Web pages but do not permit subscribers to use cgi scripts. (Olsen Test., Tr. at 345) For Web content providers who lack access to cgi scripts, there is no means of age verification.

Although some Web providers can query the user of a site for a credit card number, the cost of verification is significant, ranging from sixty cents per transaction to more than a dollar per transaction. (*Id.* at 341-42) To take advantage of adult access code or adult identification code verification, a content provider would either have to establish and maintain a registration and verification system (or hire someone else to do so) and issue access codes to users—after verifying their ages—or associate with one of several adult verification services, such as Adult Check, Adult Verification System, First Virtual, Validate, or VeriSign. (Olsen Decl. ¶ 86 & Ex. I; Schmidt Test., Tr. at 203-14; Defendant's Exs. 6, 7, 8 & 9) Although neither of the Government's expert witnesses had any first-hand familiarity with adult verification services, advertising materials suggest that an adult can obtain an identification number from a particular service and access any site registered with the service. For example, a user can register with Adult Check for an annual fee of $9.95; when the user attempts to access any site registered with Adult Check, the user is prompted to enter an Adult Check identification number that is checked against the service's database. (Defendant's Ex. 6, at 1) If the number is valid, the user is automatically admitted to the site. (*Id.*) Although most verification services do not charge content providers to register their sites (*Id.* Exs. 6-8), at least one service does impose a fee on site owners registered with it. (*Id.* Ex. 9, at 1)

Having explored various means of Internet communication, the availability and accessibility of sexually explicit content, the development of blocking software and rating schemes designed to enable

parents to shield their children from inappropriate material, and the potential for tagging and verification procedures that content providers can themselves employ in an effort to shield minors from sexually explicit content that they provide, we turn to the governmental regulation in question.

III. DISCUSSION

47 U.S.C. § 223(d), as added by the CDA, targets persons who send or display material that, "in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs." The language of § 223(d) parallels the definition of "indecency" adopted by the FCC in 1975 in the broadcast context,[14] *see FCC v. Pacifica Found.*, 56

---

[14] The FCC's definition of "indecency" in turn has its roots in the Supreme Court's obscenity jurisprudence. Under *Miller v. California*, 413 U.S. 15, 24, 93 S.Ct. 2607, 2615, 37 L.Ed.2d 419 (1973), a work is legally obscene if it "portray[s] sexual conduct in a patently offensive way" and, taken as a whole, "appeal[s] to the prurient interest in sex" and lacks "serious literary, artistic, political, or scientific value." Under the FCC's indecency definition, a work need not appeal to the prurient interest or lack serious value to be "indecent." *See Denver Area Consortium*, — U.S. at ——, 116 S.Ct. at 2389-90 (plurality opinion). We note that § 223(d) contains no reference to "indecent" speech, but merely imports the FCC's definition of indecency to define covered speech. Section 223(a)(1)(B) of the CDA, not challenged by the plaintiff in this litigation, uses the term "indecent." Like the parties in this case, we use the terms "indecent" and "patently offensive" interchangeably. The three judges in the Philadelphia litigation accepted, for purpose of adjudication of the plaintiff's motion for preliminary injunctive relief, that § 223(a)(1)(B) and § 223(d) cover the same content, despite Congress's use of the term "indecent" in one provision and the "patently offensive"

F.C.C.2d 94, 98 (1975); an application of this definition to a radio broadcast of the deliberately provocative George Carlin "Filthy Words" monologue was upheld by the Supreme Court in *FCC v. Pacifica Found.*, 438 U.S. 726, 751, 98 S.Ct. 3026, 3041, 57 L.Ed.2d 1073 (1978). Following *Pacifica*, the FCC applied the indecency standard only narrowly—taking no enforcement action unless material "involved the repeated use, for shock value, of words similar or identical to those satirized in the Carlin . . . monologue"—with the result that no broadcasts were found actionable between 1975 and 1987. *Action for Children's Television v. FCC* ("*ACT I*"), 852 F.2d 1332, 1338, 1336 (D.C.Cir.1988) (internal quotation marks omitted). In 1987, however, the FCC, in three rulings in the broadcast context, interpreted its indecency standard more broadly, extending it beyond the particular language at issue in *Pacifica*. *See Infinity Broadcasting Corp.*, 2 F.C.C.R. 2705 (1987); *Regents of the University of California*, 2 F.C.C.R. 2703 (1987); *Pacifica Found., Inc.*, 2 F.C.C.R. 2698 (1987).[15] The same standard was imported, by statute and by regulation, into other contexts, and applies to commercial telephone messages, *see Dial Info. Servs. Corp. v. Thornburgh*, 938 F.2d 1535, 1540-41 (2d Cir.1991) (quoting Regulations Concerning Indecent Communications by Telephone, 5 F.C.C.R 4926, 4927

---

description in the other. *See ACLU/ALA*, 929 F Supp. at 850 (Sloviter, C.J.), at 860 (Buckwalter, J.), at 868 (Dalzell, J.).

[15] In reviewing these rulings, the U.S. Court of Appeals for the District of Columbia Circuit approved of the more expansive interpretation of the indecency standard, *see ACT I*, 852 F.2d at 1338-40, but vacated *Regents of the University of California and Pacifica Foundation, Inc.* on other grounds, *see id.* at 1341.

(1990)), *cert. denied*, 502 U.S. 1072, 112 S.Ct. 966, 117 L.Ed.2d 132 (1992), and cable programming, *see* 47 U.S.C. § 532(h); 47 C.F.R. §§ 76.701(g), 76.702 (1995); *Alliance for Community Media v. FCC* ("*Alliance*"), 56 F.3d 105, 129 (D.C.Cir.1995) (in banc), *aff'd in part and rev'd in part sub nom. Denver Area Consortium*, — U.S. ——, 116 S.Ct. ——, — L.Ed.2d —— (1996).

The plaintiff claims principally that § 223(d), as added by the CDA, is unconstitutional on its face because it is vague and substantially overbroad. Where a plaintiff seeks to "stay government action taken in the public interest pursuant to a statutory or regulatory scheme," he must demonstrate a likelihood of success on the merits of his claims and that he will suffer irreparable harm in the absence of an injunction. *Able v. United States*, 44 F.3d 128, 131 (2d Cir.1995) (per curiam) (internal quotation marks omitted). It is well settled that "[t]he loss of First Amendment freedoms, for even minimal periods of time, unquestionably constitutes irreparable injury." *Elrod v. Burns*, 427 U.S. 347, 373, 96 S.Ct. 2673, 2690, 49 L.Ed.2d 547 (1976) (plurality opinion). Accordingly, a finding of irreparable harm flows from a court's conclusion that a governmental regulation has a chilling effect on free expression. We examine the plaintiff's vagueness and overbreadth challenges in turn.

A. *Vagueness*

We consider first the plaintiff's claim that § 223(d) is unconstitutionally vague—that it fails to convey to persons of ordinary intelligence reasonable notice of what conduct is prohibited and creates a danger of

arbitrary and discriminatory enforcement. *See Grayned v. City of Rockford*, 408 U.S. 104, 108-09, 92 S.Ct. 2294, 2298-99, 33 L.Ed.2d 222 (1972). Where a federal statute or regulation fails to supply a fair warning of what will give rise to criminal liability, it violates the Due Process Clause of the Fifth Amendment; where a statute or regulation purports to limit freedom of expression, its vagueness will also "operate[ ] to inhibit the exercise" of that freedom and violate the First Amendment. *Id.* (internal quotation marks omitted).

As previously noted, § 223(d) essentially codifies the FCC definition of indecency sustained in a particular factual context by the Supreme Court in *Pacifica*. Although the *Pacifica* Court never specifically addressed whether the FCC's definition was unconstitutionally vague, the Court's conclusion that the broadcast at issue in *Pacifica* was "indecent" and the fact that the Court quoted elements of the FCC's indecency definition with approval, *see* 438 U.S. at 739, 98 S.Ct. at 3035, has been read to foreclose a vagueness challenge to the FCC's definition for indecency in the broadcast medium. *See ACT I*, 852 F.2d at 1339-40 ("[I]f acceptance of the FCC's generic definition of 'indecent' as capable of surviving a vagueness challenge is not implicit in *Pacifica*, we have misunderstood Higher Authority and welcome correction."); *see also Action for Children's Television v. FCC*, 932 F.2d 1504, 1508 (D.C.Cir.1991) ("*ACT II*"), *cert. denied sub nom. Children's Legal Found. v. Action for Children's Television*, 503 U.S. 913, 112 S.Ct. 1281, 117 L.Ed.2d 507 (1992); *Action for Children's Television v. FCC*, 58 F.3d 654, 659 (D.C.Cir.1995) (in banc) ("*ACT III*"), *cert. denied sub*

nom. Pacifica Found. v. FCC, — U.S. ——, 116 S.Ct. 701, 133 L.Ed.2d 658 (1996). Relying on the reasoning of *Pacifica* and *ACT I*, the courts of appeals have found vagueness challenges to analogous FCC definitions reaching commercial telephone communications and cable programming unavailing. *See Dial Info. Servs.*, 938 F.2d at 1540-41 (indecent commercial telephone messages); *Information Providers' Coalition for the Defense of the First Amendment v. FCC*, 928 F.2d 866, 874-76 (9th Cir.1991) (same); *Alliance*, 56 F.3d at 129 (cable programming). Most recently, the *Alliance* court's approach on this question was affirmed by a plurality of the Supreme Court. *Denver Area Consortium*, — U.S. at ——- - ——, 116 S.Ct. at 2389-90, — L.Ed.2d — —.

In light of Supreme Court and other precedent rejecting claims that the language used by the FCC to define indecency is unconstitutionally vague, we cannot conclude that the plaintiff has demonstrated a likelihood of success on his claim that the incorporation of a virtually identical verbal formula into § 223(d) renders that statute fatally vague. The plaintiff appears to concede that a challenge based solely on the "patently offensive" language is foreclosed, but calls our attention to other purported defects in the statutory language. First, the plaintiff contends that assessment of a work's "context" in determining whether it is "patently offensive" is highly unpredictable and subjective. (Plaintiff's Memorandum of Law, filed Feb. 17, 1996, at 23) Second, § 223(d) requires content providers to judge what content will and will not subject them to criminal liability by reference to the "standards" of

an unidentified or fictitious "community." (Plaintiff's Post-Hearing Memorandum of Law ("Plaintiff's Post-Hearing Memo."), filed May 21, 1996, at 37) We conclude that neither argument supports a conclusion that § 223(d) is unconstitutionally vague. In addition, we address briefly the basis for our disagreement with the contrary conclusion reached by two of the judges in the Philadelphia litigation.

We first address the inclusion in § 223(d) of the phrase "in context." While the FCC definition that has been applied to television broadcasting since 1987—the subject of unsuccessful vagueness challenges—has included this phrase, *see Infinity Broadcasting Corp.*, 2 F.C.C.R. at 2705, definitions employed by the FCC with respect to other media have not explicitly included this phrase. *See Dial Info. Servs.*, 938 F.2d at 1540 (indecent commercial telephone messages); *Information Providers' Coalition*, 928 F.2d at 869 (same); *Alliance*, 56 F.3d at 105 (cable programming). Nevertheless, an assessment of a work's context has always been a component of indecency analysis regardless of the medium; the incorporation of the phrase "in context" merely follows the approach of *Pacifica* and later cases. *See Pacifica*, 438 U.S. at 744, 98 S.Ct. at 3037-38 (plurality opinion); *id.* at 750, 98 S.Ct. at 3041 (majority opinion); *Information Providers' Coalition*, 928 F.2d at 876; *cf. ACT I*, 852 F.2d at 1340 (discussing relevance of social value of material as factor in determining whether material is patently offensive); S.CONF.REP. 230, 104th Cong., 2d Sess. 189 ("The gravamen of the indecency concept is 'patent offensiveness.' Such a determination cannot be made without a consideration of the context of the description or depiction at

issue."). We cannot see how importing certain language that has been used by various courts considering challenges to the definition of indecency renders the CDA unconstitutionally vague.

The plaintiff's second point concerns the ability (or inability) of an Internet content provider to assess what "community standards" govern the transmission or display of patently offensive materials. A communication posted by an individual in New York City to a Usenet server and thereby made available to countless subscribers around the world might indisputably fall outside the scope of what is "indecent" by the standards of New York City, but might subject the individual to criminal prosecution in other federal districts. Nevertheless, in light of the fact that modern communications have long transcended community borders, this problem is not a novel one. Indeed, the definition of obscenity requires a publisher or distributor of arguably obscene material to look to contemporary community standards in various localities into which materials are distributed. *See, e.g., Sable Communications of California, Inc. v. FCC*, 492 U.S. 115, 125-26, 109 S.Ct. at 2836-37 (1989) (concluding that failure to apply uniform national standard of obscenity does not render statute unconstitutional; "If [the provider's] audience is comprised of different communities with different local standards, [the provider] ultimately bears the burden of complying with the prohibition on obscene messages."); *see also Miller*, 413 U.S. at 24, 93 S.Ct. at 2615 (holding that factfinder's inquiry in obscenity context focuses in part on whether "the average person, applying contemporary community standards, would find that the work, taken as a whole,

appeals to the prurient interest" (internal quotation marks omitted)).

The plaintiff attempts to distinguish past cases rejecting vagueness challenges to indecency definitions incorporating "community standards" language on two grounds. First, the plaintiff contends that Internet content providers are less well equipped to assess community indecency standards than those within the reach of previous statutes and regulations governing indecency; while entities engaging in the commercial traffic of pornographic materials (such as obscene or indecent telephone messages) may have legal staff to monitor FCC pronouncements on what is and is not patently offensive in communities across America, we are told, individuals engaged in an exchange of ideas over the Internet do not. (Oral Argument, June 3, 1996, Tr. at 24-25) Second, the plaintiff claims that even if those who use other communications media can tailor their messages to a particular community—as suggested by the Supreme Court in *Sable Communications*—Internet content providers simply cannot restrict the geographic area within which their messages are received. (Plaintiff's Post-Hearing Memo. at 39)

We are not persuaded. The plaintiff has offered no authority for the proposition that, so long as the providers of content targeted by a statute are private individuals, Congress cannot constitutionally link proscribed conduct to the community standards of various localities. While it is true that congressional action has directly targeted *commercial* dial-a-porn services, and restrictions on indecency in radio and television broadcasting or cable programming mainly affect for-profit enterprises, liability for violation of

indecency restrictions has not been tied to the ability of a content provider to marshal its resources to explore various community indecency standards. Distributors of allegedly obscene materials may also be subjected to varying community standards; we know of no exemption for individuals whose primary motive is non-economic. Due process requires that a criminal statute "give the person of ordinary intelligence a reasonable opportunity to know what is prohibited, so that he may act accordingly," *Grayned*, 408 U.S. at 108, 92 S.Ct. at 2298-99; it does not require "mathematical certainty," *id.* at 110, 92 S.Ct. at 2300, or " 'impossible standards' of clarity," *Kolender v. Lawson*, 461 U.S. 352, 361, 103 S.Ct. 1855, 1860, 75 L.Ed.2d 903 (1983) (quoting *United States v. Petrillo*, 332 U.S. 1, 7-8, 67 S.Ct. 1538, 1541-42, 91 L.Ed. 1877 (1947)). We have no basis for concluding that Internet content providers are any less capable than those subject to obscenity laws or other indecency restrictions to acquire a general familiarity with the relevant standards; indeed, one might conclude that a content provider's contact with others around the country and around the world through interactive computer services would cultivate a heightened awareness of regional and cultural differences.

We turn to the plaintiff's claim that, even assuming a content provider can discern the appropriate community standards, the provider has no choice but to gear his message toward the least tolerant community. More specifically, unlike a provider of obscene or indecent telephone communications or cable programming, who might be able to prevent a message from being transmitted to certain geographical areas, an Internet content provider has no

way of identifying the receiving community. It follows that, to comply with the CDA, a content provider must take steps to limit minors' access to *all* material that would be considered patently offensive in *any* community; only then could the content provider be sure that material considered inappropriate under the standards of a particular community is not available to minors in that community.

The problem that the plaintiff presents appears to raise questions of overbreadth rather than vagueness. In light of our other conclusions *infra* and in the absence of even a preliminary showing in this record by either party regarding distinctions in community standards, we decline to address whether any overbreadth in this respect is "substantial."

As noted, two of the judges in the Philadelphia litigation concluded that the provision of the CDA challenged by the plaintiff is unconstitutionally vague. That conclusion rests in part on the fact that the indecency definitions upheld in past cases defined indecency by reference to community standards *for a particular medium*. For example, the FCC definition of indecency upheld in *Dial Info. Servs.*, 938 F.2d at 1540, contained a reference to what is patently offensive as measured by contemporary community standards "for the telephone medium." *See ACLU/ALA*, 929 F.Supp. at 862 (Buckwalter, J.). We can find no authority discussing the significance of the definition's reference to the telephone medium or of analogous references to the broadcast or cable media.[16] Particularly in light of the fact that no court

---

[16] Indeed, the statutory definition of indecency for the cable medium, found not to be vague by a plurality of the Court in

addressing an indecency challenge has focused on any of these references, it is unclear how *Pacifica* and its progeny can be thought to require its existence, or how the absence of a reference to the particular communications medium targeted by the CDA renders the statute unconstitutionally vague.

Finally, we address the slightly different argument raised by the same two judges in the Philadelphia litigation—that the CDA is vague not only because it fails to provide the requisite guidance to those seeking to avoid criminal liability, but also because it leaves open the possibility of arbitrary enforcement. This conclusion stems in part from the Government's apparent representation in that case that the challenged provisions of the CDA will be applied only to "pornographic" material. We note that the Government has made no such representation here, and clearly contemplates the application of the CDA to material that is patently offensive although not necessarily pornographic. While we are properly required to approach the question of whether a criminal statute is vague with great skepticism that prosecutorial good faith can cure an identified defect, *see Baggett v. Bullitt*, 377 U.S. 360, 373-74, 84 S.Ct. 1316, 1323-24, 12 L.Ed.2d 377 (1964) ("Well-intentioned prosecutors and judicial safeguards do not neutralize the vice of a vague law."), we are constrained to conclude that this statute is not vague, and does not leave in the hands of prosecutors the sole discretion

---

Denver Area Consortium, makes no reference to the community standards for the cable medium. — U.S. at ——, 116 S.Ct. at 2389-90. *Compare* 47 U.S.C. § 532(h) (lacking reference to standards for cable medium) *with* 47 C.F.R. § 76.701(g) (including reference to standards for cable medium).

to delineate its contours. Congress did not fashion the "patently offensive" provision of § 223(d) out of whole cloth. To the extent that the FCC and courts have, in construing similarly worded indecency provisions against the backdrop of the First Amendment, previously drawn distinctions between serious discussions of sexual issues and material in which sexuality is portrayed in a purposefully offensive manner, Congress's choice of language in § 223(d) cabins prosecutorial discretion by incorporating FCC and court rulings reflecting those distinctions. *Compare Letter to Mr. Peter Branton*, 6 F.C.C.R. 610 (1991) (dismissing indecency complaint regarding radio news story including broadcast of wiretap in which John Gotti repeatedly used an expletive; concluding that "the program segment, when considered in context, was an integral part of a *bona fide* news story concerning organized crime"); *In re King Broadcasting Co.*, 5 F.C.C.R. 2971 (1990) (dismissing indecency complaint regarding broadcast of program "Teen Sex, What About the Kids?"; concluding that "[a]lthough the program dealt with sexual issues, the material presented was clinical or instructional in nature and not presented in a pandering, titillating or vulgar manner or in any way that we would consider patently offensive"), *with In re Sagittarius Broadcasting Corp.*, 7 F.C.C.R. at 6874 (upholding finding of indecency with respect to broadcast making "frequent, explicit, patently offensive references to sexual intercourse, orgasm, masturbation, and other sexual conduct, as well as to breasts, nudity, and male and female genitalia"). Enforcement of § 223(d) does not depend upon prosecutorial whim, but upon prosecutorial fidelity to distinctions that Congress sought, through codification of a definition of in-

decency that has been authoritatively construed for a variety of media in recent years, to incorporate into the CDA. *See* S.CONF.REP. 230, 104th Cong., 2d Sess. 189 (1996).

In sum, we conclude that the plaintiff has not shown a likelihood of success on the merits of his claim that § 223(d) is unconstitutionally vague.

B. *Substantial Overbreadth*

The plaintiff also claims that § 223(d) is substantially overbroad and therefore facially invalid. The doctrine of overbreadth recognizes that an unconstitutional restriction of freedom of expression may deter parties not before the court from engaging in protected speech and thereby escape judicial review. *See Broadrick v. Oklahoma*, 413 U.S. 601, 612-13, 93 S.Ct. 2908, 2916-17, 37 L.Ed.2d 830 (1973); *Gooding v. Wilson*, 405 U.S. 518, 520-21, 92 S.Ct. 1103, 1105-06, 31 L.Ed.2d 408 (1972). Accordingly, an overbreadth challenge can be raised "with no requirement that the person making the attack demonstrate that his own conduct could not be regulated by a statute drawn with the requisite specificity." *Dombrowski v. Pfister*, 380 U.S. 479, 486, 85 S.Ct. 1116, 1120, 14 L.Ed.2d 22 (1965). That is, even if a statute could be validly applied to the plaintiff and others, it may be so broad as to inhibit the constitutionally protected speech of third parties not before the Court. Invalidation of a statute on overbreadth grounds is "strong medicine," and is inappropriate unless the overbreadth is substantial and no limiting construction could be placed upon the challenged statute. *Broadrick*, 413 U.S. at 613, 615, 93 S.Ct. at 2916, 2917-18; *see also Forsyth County v. Nationalist*

Movement, 505 U.S. 123, 130, 112 S.Ct. 2395, 2401, 120 L.Ed.2d 101 (1992) (noting that Court has permitted overbreadth challenges "where [a statute] sweeps too broadly, penalizing a substantial amount of speech that is constitutionally protected"); *New York State Club Ass'n v. City of New York*, 487 U.S. 1, 11, 14, 108 S.Ct. 2225, 2233, 2234-35, 101 L.Ed.2d 1 (1988) (noting that an overbreadth challenge is justified only if "a substantial number of instances exist in which [the statute] cannot be applied constitutionally"); *City of Houston v. Hill*, 482 U.S. 451, 458, 107 S.Ct. 2502, 2508, 96 L.Ed.2d 398 (1987) ("[In an overbreadth challenge], a court's first task is to determine whether the enactment reaches a substantial amount of constitutionally protected conduct." (internal quotation marks omitted)); *Members of the City Council v. Taxpayers for Vincent*, 466 U.S. 789, 801, 104 S.Ct. 2118, 2126, 80 L.Ed.2d 772 (1984) (noting that an overbreadth challenge will succeed only if there is "a realistic danger that the statute itself will significantly compromise recognized First Amendment protections of parties not before the Court").

Applying these principles, we must determine whether § 223(d) unconstitutionally restricts freedom of expression, and, if so, whether the statute criminalizes a category of protected speech that is substantial in relation to the category that could legitimately be proscribed. Section 223(d) constitutes a content-based regulation of speech; in most contexts, such a regulation would be subject to the strictest judicial scrutiny and therefore would be impermissible absent a showing that the regulation is supported by a compelling interest and is narrowly tailored to achieve that interest. *See Sable Communications*,

492 U.S. at 126, 109 S.Ct. at 2836-37. At oral argument, the Government's counsel conceded that strict scrutiny analysis is appropriate for purposes of this Court's adjudication of the plaintiff's motion for preliminary injunctive relief: nonetheless, we pause to consider this question in greater detail in light of the Supreme Court's recent decision in *Denver Area Consortium*, — U.S. ——, 116 S.Ct. 2374. There a plurality of the Court assessed the constitutionality of statutory provisions (1) granting cable operators the power to prohibit indecent communications on "leased access channels"—*i.e.*, channels reserved under federal law for commercial lease by unaffiliated third parties; (2) requiring cable operators to segregate and block indecent programming if they decide to permit, rather than to prohibit, its broadcast; and (3) granting cable operators the power to prohibit indecent programming on "public access channels"—*i.e.*, channels reserved under local franchise agreements for public, educational, or governmental purposes. *Id.* at —— - ——, 116 S.Ct. at 2380-82. Recognizing that the Court's First Amendment jurisprudence involved application of principles tailored to different communications media, the plurality expressly declined to adopt a definitive standard for evaluating content-based regulation in the cable medium to apply in all future circumstances. *Id.* at ——, 116 S.Ct. at 2385. Accordingly, the plurality did not evaluate the restrictions on indecent cable broadcasts under a standard of "strict scrutiny," but rather assessed whether the restrictions "properly addresse[d] an extremely important problem, without imposing, in light of the relevant interests, an unnecessarily great restriction on speech." *Id.* at ——, 116 S.Ct. at 2385.

As the *Denver Area Consortium* plurality itself recognized, there was little difference between the standard it applied and the strict scrutiny approach that Justice Kennedy endorsed in his partial concurrence. *See id.* at ——, 116 S.Ct. at 2387. We have no doubt, however, that strict scrutiny should apply here. The plurality's decision not to expressly apply strict scrutiny in *Denver Area Consortium* depended in part on the likelihood that children would be exposed to indecent cable programming; reasoning that, like broadcast television or radio, cable television is "uniquely pervasive" in homes and highly accessible to children and that patently offensive material confronts the viewer "with little or no prior warning," the plurality reasoned that *Pacifica*'s consideration of a limitation on indecent broadcasting was persuasive. *Id.* at ——, 116 S.Ct. at 2386-87 (internal quotation marks omitted). The plurality distinguished *Sable Communications* in part because it "involved a communications medium, telephone service, that was significantly less likely to expose children to [indecent] material, was less intrusive, and allowed for significantly more control over what comes into the home." *Id.* at ——, 116 S.Ct. at 2388. As our findings of fact make clear, it takes several affirmative steps for a user to gain access to material through an interactive communications service. Indecent content on the Internet ordinarily does not assault a user without warning: a child cannot gain access to Internet content with the touch of a remote control, and while accidental viewing of indecent content is possible, there is no evidence in this record to suggest that it is likely. Accordingly, we find strict scrutiny appropriate here.

In charging that § 223(d) unconstitutionally restricts protected expression, the plaintiff pursues two distinct arguments. First, the plaintiff contends that § 223(d) reaches a significant amount of Internet content with serious literary, artistic, political, or scientific value, and that the government cannot demonstrate any compelling interest in restricting the availability of such material on the Internet. Second, the plaintiff claims that § 223(d) (considered together with certain affirmative defenses to criminal liability set forth in § 223(e)(5)) is not narrowly tailored, in that it fails to preserve for adults the ability to engage in certain constitutionally protected communications—effectively acting as a total ban on indecent communications by interactive computer systems.

We find it necessary to address only the second of these claims. Entirely independently of the question of whether matter of serious value is chilled by the CDA, the statute constitutes an overly broad restraint on protected communication between and among adults. Of course, the statute would be even more constitutionally defective if it encompassed work of serious value that the government has no compelling interest in regulating. In light of our finding on the plaintiff's second overbreadth claim, however, it is unnecessary to resolve the question of whether he has demonstrated a likelihood of success on his claim that the CDA would proscribe a substantial body of work that is of serious value but that is not harmful to minors and therefore not in the government's compelling interest to regulate. *Broadrick*, 413 U.S. at 615, 93 S.Ct. at 2917-18.

It is also unnecessary, given our holding on the plaintiff's second overbreadth claim, to decide whether the potential ineffectiveness of the CDA in eradicating the problem of minors' having access to sexually explicit material on the Internet renders the statute constitutionally defective. Because the CDA only regulates content providers within the United States, while perhaps as much as thirty percent of the sexually explicit material on the Internet originates abroad, *see* findings of fact, *supra*, at p. 929, the CDA will not reach a significant percentage of the sexually explicit material currently available. Considering, as we hold below with respect to the plaintiff's second overbreadth claim, that the CDA can be expected to chill the First Amendment rights of adults to engage in the kind of expression that is subject to the CDA's criminal penalties, the apparent ineffectiveness of the CDA underscores our holding today that the Government has failed to demonstrate that the CDA does not "unnecessarily interfer[e] with First Amendment freedoms." *Sable Communications*, 492 U.S. at 126, 109 S.Ct. at 2836 (internal quotation marks omitted). Even if it were established that the statute is to some limited extent effective in protecting minors from sexually explicit material on line, and that nothing short of a total ban on indecent communication could be as effective, it is not obvious that the benefits thus achieved would outweigh the burden, described below, imposed on the First Amendment rights of adults. As our Court of Appeals has repeatedly stated, "[T]he State may not regulate at all if it turns out that even the least restrictive means of regulation is still unreasonable when its limitations on freedom of speech are balanced against the benefits gained from those limitations." *Carlin*

Communications, Inc. v. FCC, 837 F.2d 546, 555 (2d Cir.) (internal quotation marks omitted), *cert. denied*, 488 U.S. 924, 109 S.Ct. 305, 102 L.Ed.2d 324 (1988).

We turn now to the plaintiff's second overbreadth claim, analytically distinct from the first, that the CDA acts as a ban on certain constitutionally protected communications between adults. For purposes of our discussion of this claim, we will assume that the government has a compelling interest in restricting minors' access to all (or virtually all) "patently offensive" material—that is, that all such material is found to be harmful to minors. The question is whether the challenged provision of the CDA is a "narrowly drawn regulation[ ] designed to serve [the government's] interest[ ] without unnecessarily interfering with First Amendment freedoms." *Sable Communications*, 492 U.S. at 126, 109 S.Ct. at 2836 (internal quotation marks omitted). The plaintiff claims that the statute fails to safeguard for *adults* the means of engaging in constitutionally protected communications through interactive computer services.

The Government concedes that § 223(d), standing alone, is not constitutionally defensible. (Oral Argument, June 3, 1996, Tr. at 69-71) As discussed in greater detail in our factual findings, and as the Government concedes, for the vast majority of applications and services available on the Internet, a user has no way of communicating or making available patently offensive content with certainty that the content will not reach a person under eighteen years of age. (*See* Findings of Fact, *supra*; Oral Argument, June 3, 1996, Tr. at 69) For example, an individual sending a message that will be retrans-

mitted by a mail exploder program has no way of knowing the identity of other subscribers (even if he knows the e-mail address of each subscriber). A content provider has no way of knowing who will have access to an article posted to a Usenet newsgroup. Individual participants in an Internet Relay Chat discussion know other participants only by the names they choose upon entering the discussion; users can participate anonymously by using a pseudonym. A content provider who makes files available on an anonymous FTP or on a gopher or Web server has no way of knowing the identity of other participants who will have access to those servers.

Because content providers using most forms of Internet communication have no way of transmitting indecent content with certainty that it will not reach a minor, the only way for a content provider to comply with § 223(d), standing alone, would be to refrain from transmitting any indecent content. Because adults would lack means of engaging in constitutionally protected indecent communications over the Internet without fear of criminal liability, the statute would unquestionably be unconstitutional. *See Sable Communications*, 492 U.S. at 131, 109 S.Ct. at 2839 (holding that total ban on commercial indecent telephone messages "has the invalid effect of limiting the content of adult telephone conversations to that which is suitable for children to hear").

Section 223(d), however, does not stand alone. In § 223(e)(5), Congress supplied two affirmative defenses to liability under the CDA. First, § 223(e)(5)(A) provides that it is a defense to a prosecution under § 223(d) that a person "has taken, in good faith, reasonable, effective, and appropriate actions under

the circumstances to restrict or prevent access by minors to [covered] communication[s], which may involve any appropriate measures to restrict minors from such communications, including any method which is feasible under available technology." Second, § 223(e)(5)(B) provides that it is a defense to a prosecution under § 223(d) that a person "has restricted access to [covered] communication[s] by requiring use of a verified credit card, debit account, adult access code, or adult personal identification number." Accordingly, our inquiry is whether the statutory defenses adequately ensure that would-be speakers can use the Internet to transmit constitutionally protected communications to adults. The Government concedes that it bears the burden of proving that § 223(d), taken together with the statutory defenses, preserves the ability of adult Internet speakers to engage in constitutionally protected indecent communications (Oral Argument, June 3, 1996, Tr. at 28-29), *see R.A.V. v. City of St. Paul*, 505 U.S. 377, 382, 112 S.Ct. 2538, 2542, 120 L.Ed.2d 305 (1992) (noting that content-based regulations are presumptively invalid); only if adults can engage in such communications can the court conclude that the relevant provisions of the CDA are narrowly tailored to achieve the government's interest in restricting minors' access to indecent material. We examine the § 223(e)(5) defenses in reverse order.

1. *Verified Credit Card, Debit Account, Adult Access Code, or Adult Identification Number*

The Government does not claim that § 223(e)(5)(B) serves as a defense for content providers using all or even most forms of on-line communication. If a

content provider cannot discern who receives his messages, there is no way for him to obtain verification of recipients' ages. As previously noted, a speaker posting a message to a newsgroup or to a list maintained by a mail exploder has no control over who will receive the message; a user who joins an IRC discussion channel cannot determine the identity of other participants, beyond viewing a list of names. Because speakers wishing to use these forms of communication have no way of identifying the recipients of their messages, they simply cannot seek to obtain any credit card or access code verification of a recipient's age. Similarly, credit card or adult access verification is not available as a defense to content providers who maintain FTP servers and wish to permit "anonymous" access to files or who maintain gopher servers.[17]

As previously explained, evidence adduced at the three-day hearing suggests that some form of verification is technologically feasible for at least one mode of on-line communication relevant for our purposes: the World Wide Web. *See* Findings of Fact, *supra*, at pp. 930-931. Based on this evidence of record, it is possible to conclude that § 223(e)(5)(B) serves as an adequate defense for at least certain

---

[17] We note that an FTP server can be configured to verify a password against a list of passwords issued to users maintaining an account on the server before permitting access to certain files. A provider opting for such a configuration, however, would not be able to make files falling within the scope of the CDA broadly available to "anonymous" adult users—*i.e.*, users without an account on the system. Moreover, such a configuration is impracticable insofar as it requires the maintenance of an extensive database of authorized user names and passwords.

commercial providers of Web content-specifically, those who primarily make Web content available for "purchase" or, put another way, those who charge Web users to gain access to, and view, their content. Many commercial content providers charge a fee to permit a user to gain access to sexually explicit content, thus necessitating credit card verification in any event. Nevertheless, we note that the category of "commercial content providers" is itself somewhat elusive, and it is not clear that all content providers who could be termed "commercial" content providers could absorb the cost of credit card verification. Consider, for example, a software developer who makes a program available on line for users to download (that is, copy to the hard drive of the user's computer) without charge, for a short trial period, with the understanding that the user will remit a registration fee if the user decides to retain the program after the trial period. Although the software developer has a commercial purpose, it is not clear that he could bear the economic burden of verifying the credit cards of all those who access his software (as opposed to those who ultimately enter into a licensing agreement).

Were § 223(e)(5)(B) the only defense available to providers of Internet content, the conclusion would be inescapable that the provision challenged by the plaintiff reaches a substantial amount of protected speech and is therefore constitutionally infirm. For speakers using most Internet applications—e-mail, newsgroups, chat rooms—§ 223(e)(5)(B) is no defense at all; to avoid the threat of CDA liability, they would simply have to refrain from engaging in constitutionally protected speech. For non-commercial

content providers and possibly some commercial providers, credit card verification or maintenance of a verification system would be extremely costly. The Government urges that all Web content providers—commercial and non-commercial alike—could associate with "adult verification services." This argument ignores what is obvious from examining the advertisements and informational literature in the record regarding such services: these services are used in connection with, and indeed gear their promotional materials toward, so-called "adult" sites offering pornographic images and users of such sites. We have no doubt that it would be burdensome for some non-commercial and commercial content providers wishing to make available other types of material arguably falling within the scope of the CDA, and for users wishing to retrieve such material, to associate with "adult verification services."

2. *Good-Faith Defense*

We turn, then, to § 223(e)(5)(A), which provides a defense to CDA liability for content providers who, "in good faith," take "reasonable, effective, and appropriate actions under the circumstances," including any steps "feasible under available technology" to prevent minors' access to communications falling within the scope of the CDA. The Conference Report accompanying the CDA emphasizes that the term "effective" is to be given "its common meaning and does not require an absolute 100% restriction of access to be judged effective." S.CONF.REP. NO. 230, 104th Cong., 2d Sess. 190 (1996).

Although the statute does not require that a content provider take steps that are one-hundred

percent effective in restricting minors' access to indecent communications, it is not disputed that § 223(d) cannot stand unless there *are* reasonably effective means of ensuring that covered communications do not reach minors. (Oral Argument, June 3, 1996, Tr. at 69-71; *see supra* p. 936) While the statute makes clear that a content provider is permitted to do anything that is "feasible" under current technology to restrict minors' access to covered communications, it does not by its terms allow content providers to escape liability if there is no feasible and reasonably effective way of limiting minors' access to those communications. Throughout this litigation, the Government has attempted to identify certain steps—nowhere specifically set forth in the CDA—that content providers could take that would, absent extraordinary circumstances, constitute substantial evidence of a § 223(e)(5)(A) defense. On April 30, 1996, the Court directed the Government to obtain clarification of the Department of Justice position regarding the applicability of § 223(e)(5)(A). On May 3, 1996, the Government filed a letter from John C. Keeney, Acting Assistant Attorney General of the Criminal Division of the Department of Justice ("Keeney Letter"), stating in pertinent part:

> Under present technology, non-commercial content providers can take steps to list their site[s] in URL registries of covered sites, register their site[s] with the marketplace of browsers and blocking software (including listing an IP address), place their material in a directory blocked by screening software, or take other similarly effective affirmative steps to make their site[s] known to the world to allow the site[s] to be

> blocked. Under present technology, it is the position of the Department of Justice that, absent extraordinary circumstances, *such efforts would constitute substantial evidence* that a content provider had taken good faith, reasonable, effective, and appropriate actions under the circumstances to restrict or prevent access by minors to the covered material. The same would be true for tagging by content providers, *coupled with evidence that the tag would be screened by the marketplace of browsers and blocking software.*

(Emphasis supplied.) Following closing arguments on June 3, 1996, the Court ordered supplemental briefing by the Government focusing in particular on the technological feasibility and the effectiveness of some of the steps set forth in the Keeney Letter. We examine whether content providers using various forms of Internet communication can avail themselves of the good-faith defense set forth in § 223(e)(5)(A)—that is, whether § 223(e)(5)(A) enables them to engage in constitutionally protected communications without fear of criminal liability.[18]

We note at the outset that the Government has nowhere represented that the articulation of the Department of Justice's position in the Keeney Letter would prevent any United States Attorney

---

[18] This inquiry is, of course, distinct from an inquiry into whether the fact that § 223(e)(5)(A) nowhere identifies any specific steps that a content provider can take to enter its "safe harbor" renders § 223(d) unconstitutionally vague, because individuals lack sufficient notice as to how to shield themselves from criminal liability under the statute. The plaintiff does not press this argument here.

from arguing in a particular prosecution that any of the steps identified in the letter do not satisfy the requirements of § 223(e)(5)(A). In fact, it appears that in the Philadelphia litigation, where the Government was granted leave to file the Keeney Letter, the Government expressly conceded that the letter does not preclude a United States Attorney from taking a contrary position in particular litigation. *See ACLU/ALA*, 929 F.Supp. at 878 n. 20 (Dalzell, J.). In addition, neither § 223(e)(5)(A) itself nor the Government's representations concerning that section can be read to suggest that individuals taking the enumerated steps need not fear *prosecution* (as distinct from ultimate criminal liability). Section 223(e)(5)(A) (like § 223(e)(5)(B)) supplies a content provider with an affirmative defense, to be invoked after a criminal prosecution has been initiated and after the Government has presented its case; the steps specified by the Government are said to constitute "substantial evidence" of the affirmative defense. Because § 223(e)(5)(A) in no way shields a content provider from prosecution, it cannot be said that the steps enumerated by the Government eliminate any chilling effect that the "patently offensive" provision otherwise would have.

Even if we were satisfied that the Department of Justice's position regarding the scope of § 223(e)(5)(A), as stated in the Keeney Letter, could be uniformly implemented, that the Government would not prosecute individuals who had taken the enumerated steps, *and* that individual content providers' knowledge that they would not be prosecuted would eliminate any chilling effect that the challenged provision might otherwise have, we are

unavoidably constrained to conclude that § 223(e)(5)(A) does not provide a safe harbor in a substantial number of circumstances. We examine the particular steps suggested by the Government.

a. *Tagging*

We look first to the concept of "tagging," the subject of extensive testimony at the evidentiary hearing, as described above. *See* Findings of Fact, *supra*, at pp. 929-930. As one of the Government's expert witnesses testified, content providers wishing to transmit or make available material that they believe to fall within the scope of the CDA could identify the material as such by inserting a tell-tale "tag" into a site's name or address. Even assuming that content providers are able to distinguish accurately between material subject to the CDA and material not subject to the CDA, and assuming that any requirement that content providers label constitutionally protected but patently offensive communications would not lead a significant number of content providers to refrain from transmitting such communications, the tagging scheme suggested by the Government's expert still fails to bring content providers within § 223(e)(5)(A)'s safe harbor, for several reasons. The simple act of inserting a tag in the address of a domain, directory, or file; the name of a newsgroup or IRC channel; the subject line of an e-mail message or newsgroup article; or the source code of an HTML document, is completely ineffective in preventing minors' access to patently offensive materials. For a tagging scheme to be effective, the tag must be capable of being detected by server software designed to make the materials available or by client software used to request access to or to

display such materials. (Olsen Test., Tr. at 321-22) Indeed, the Government has carefully avoided representing that tagging alone constitutes "substantial evidence" that the content provider has used reasonable, effective, and appropriate means for preventing minors' access to constitutionally protected communications. Rather, the Department of Justice has indicated that, absent unusual circumstances, evidence of tagging, "*coupled with evidence that the tag would be screened by the marketplace of browsers and blocking software*," would constitute substantial evidence of compliance with § 223(e)(5)(A). (Keeney Letter at 2 (emphasis supplied)) The evidence adduced at the hearing, however, indicates that there is currently no tag (such as "-L18") widely recognized as signaling that content falls within the scope of the CDA. More important, the CDA imposes no obligation on the manufacturers of browsers and blocking software to configure their products to detect a particular tag; content providers' ability to mount a tagging defense depends upon the actions of these parties, whose cooperation is not required under the Act.

Despite the lack of a recognized tag for CDA content, a content provider could presumably insert into an address a label—such as "sex" or "xxx"-designed to trigger blocking features (even in the absence of a CDA tag agreed upon by the "marketplace of browsers and blocking software" or prescribed by law). It is unclear that this step would satisfy either the terms of the government's policy as stated in the Keeney Letter or the plain language of the statute. The terms of the Keeney Letter contemplate screening by the "marketplace of browsers

and blocking software." As the Government has strenuously argued, blocking software is not in wide use today. (Defendant's Post-Hearing Memo at 54-55; *See* findings of fact, *supra* at p. 929). Accordingly, even if content providers could offer evidence that they "tagged" content within the reach of the CDA prior to displaying it, and that available *blocking software* is configured to detect the tag, it is difficult to see how their actions could be regarded as "effective" means of preventing minors from gaining access to materials.

At the hearing, the Government introduced no evidence that any *browser*—that is, client software permitting a user to view materials available on Web servers—is currently configured to detect and block access to a directory or file containing a particular string of characters. After the Court ordered the Government to file supplemental materials regarding the Keeney Letter, the Government submitted an article detailing the release of a Microsoft browser, Internet Explorer 3.0, capable of screening content based on labels compatible with PICS. (Supplemental Declaration of William J. Hoffman, Ex. C; *see* findings of fact, *supra*, at p. 930). If a content provider were to tag a file with a name incorporating a PICS label, a minor seeking access to such a file on a system running this browser (appropriately set) could not do so. (*Id.*)

The Government also points to the fact that CompuServe and Prodigy have linked their browsers to parental screening software offered by Cyber Patrol (Joint Stip. ¶ 57) and that a browser offered by InterGO Communications includes a PICS-compatible screening feature. Yet there are

numerous other browsers lacking any screening features—including Netscape Navigator, which controls some eighty percent of the browser market. (Olsen Decl. ¶ 101) A content provider simply could not show that a tag is screened by the "marketplace of browsers" when only a handful of browsers have screening capabilities. Even if it were possible to show that all browsers with screening features would detect a label, the Government has not suggested, much less proven, that browsers with such screening features are in wide use. Without such a showing, it is difficult to see how tagging could be "effective" within the meaning of § 223(e)(5)(A).

In sum, we fail to see how content providers attempting to carry a § 223(e)(5)(A) defense could do so by introducing evidence that they had tagged materials within the scope of the CDA and that browsers or blocking software in the "marketplace" can detect the tags. Without a showing that a range of browsers and blocking software capable of detecting the tag exist and are in wide use, tagging cannot be thought reasonably "effective." If it is the Government's position that a content provider need *not* show that the relevant tag is widely screened—that is, screened by the "*marketplace* of [available] browsers," not simply by a few browsers that may or may not be in wide use—it is at odds with the statutory language, which requires that content providers take *effective* means to prevent minors' access to patently offensive materials. To put the matter simply, unless and until blocking software is widely in place, or unless and until those who produce and market browsers—on whom Congress placed no obligations in the CDA—configure those browsers to

recognize particular labels, tagging to prevent minors' access to material available on the Web cannot be "effective."

We note also that "browsers" are client software designed to obtain access to material available on the World Wide Web. While some permit the user to engage in other modes of Internet communication, there is no evidence that those with screening features would restrict access to, for example, tagged newsgroups, mailing lists, and chat rooms. One of the Government's two expert witnesses testified that client software enabling users to read e-mail and newsgroups, as manufactured and distributed, is not configured to supply users with options to detect particular labels or tags in newsgroup names, e-mail addresses, or subject lines accompanying articles and messages. (Olsen Test., Tr. at 331, 334) Such software can, however, be reconfigured by a user to detect particular tags. (*Id.* at 331) We doubt that a content provider could rely on tagging, coupled with the fact that e-mail and newsgroup readers can reconfigure their software to detect certain tags, as evidence of reasonable and effective efforts to prevent minors' access to materials falling within the scope of the CDA. A content provider has no control over what client software a user installs, how the user reconfigures that software, or whether a minor can undo the reconfiguration. (*Id.* at 333, 334) Thus, a content provider has no way of ensuring that a message posted to a newsgroup or a mailing list will not be available to persons under the age of eighteen; to rely on the combination of tagging and client software to come within the § 223(e)(5)(A) defense, a content provider would have to assume that third

parties—namely, the users—install and reconfigure software, and would risk criminal liability if that dubious assumption proved incorrect.

b. *Placing Content in Blocked Directories and Registering Content*

Having concluded that the tagging scheme pressed by the Government does not presently offer a substantial number of content providers an affirmative defense to criminal liability under the CDA, we turn to other steps identified in the Keeney Letter.

Those steps fall roughly into two categories. First, the Keeney Letter suggests that steps taken by content providers to "place their material in a directory blocked by screening software" will constitute substantial evidence of compliance with § 223(e)(5)(A).[19] For example, a content provider can take steps to ensure that the site is listed with a directory of sites containing "adult" material, such as a section of the *Internet Yellow Pages* identifying adult materials (Hoffman Decl., Ex. 6) or a section of an on-line directory system such as Yahoo reserved for sexually explicit materials. The record suggests that screening software such as SurfWatch is

---

[19] The Keeney Letter also indicates that content providers can take steps to ensure that their sites are listed "in URL registries of covered sites." In response to the Court's request for supplemental submissions, the Government appears to suggest that "registries" are no different from "directories," and that a "covered" site is a site blocked by screening software. (Defendant's Supplemental Post-Hearing Memorandum of Law, at 1 n. 1, 2) The steps by content providers contemplated here are essentially identical to "plac[ing] . . . material in a directory blocked by screening software." (*See also* Olsen Test., Tr. at 447-48)

designed to block sites listed in the *Internet Yellow Pages* under the category "X-Rated Resources." (Stipulated Record, Ex. M, at 137-39 (Duvall Test.); *id.* Ex. Q)

Second, the Keeney Letter suggests that steps taken by content providers to "register their site[s] with the marketplace of browsers and blocking software" will constitute substantial compliance with § 223(e)(5)(A). Attempting to lend substance to this language, the Government notes that certain commercial on- line services, Internet service providers, browsers, and blocking software will block access to sites "registered" with their services. (Defendant's Supp.Memo. at 3-4) Thus, the Government contends that, "absent extraordinary circumtances," content providers who directly register their sites with an unspecified number of such companies will have satisfied § 223(e)(5)(A). (*Id.*)

Again, it appears that the Government's representation fails to help any substantial number of content providers to enter the safe harbor offered by § 223(e)(5)(A). As previously noted, the Government has offered no evidence, and does not contend, that the products and services that offer to block site access cover even a significant portion of the available market. If that portion were not significant, site registration would accomplish little, and would certainly not serve as an "effective" means to restrict the access of minors to Internet content. Similarly, the effectiveness of securing a listing in a directory containing sexually explicit sites depends upon households' voluntary use of blocking software. The Government strenuously argues—and we have found—that blocking software is not widely used (De-

fendant's Post-Hearing Memo. at 54-55; *see* findings of fact, *supra*, at p. 929), and content providers certainly cannot cause its greater use.

We note in passing two additional steps for compliance with § 223(e)(5)(A) offered by the Government but not included in the Keeney Letter. The Government suggests that those *adults* who wish to exchange indecent communications can do so by confining those communications to limited membership or limited access forums. For example, an adult user could post indecent e-mail only to "closed" mailing lists, whose subscribers could be "approved" based on age. As previously noted, however, an e-mail address provides no authoritative information about a subscriber; an individual managing a "closed" mailing list would have to use some other means of identifying subscribers' ages. The Government suggests none; presumably, the list manager could obtain a credit card number from each subscriber. Again, however, verification would be costly, and not likely an option for a non-commercial content provider.

The Government also urges that content providers could post indecent material to limited newsgroups. A newsgroup cannot be limited in the same sense as a mailing list; communications are not transmitted from a central server, but are passed among servers participating in the Usenet system. Accordingly, a limited newsgroup is achieved by restricting the number of servers on which posted articles appear.

Although the concept is not well developed in the record, it is clear that the server or servers on which the newsgroup is available would need the capacity to verify that any user requesting access to an article is

an adult. (Olsen Decl. ¶¶ 75-87 (describing concept of a "verified server")) The Government's suggestion assumes that users will possess the resources and expertise to establish and maintain a server; although several individuals or entities could share a single server, the record suggests that the cost of establishing a server is not trivial-indeed, the price could range beyond three-thousand dollars. (Galligher Test., Tr. at 182 (describing cost of maintaining mail server))

In sum, there is no persuasive evidence that a substantial proportion of Internet content providers can make available material potentially within the scope of the CDA without fear of prosecution and criminal liability. Leaving aside the fact that § 223(e)(5) sets forth affirmative defenses—and thus offers no assurance that a content provider will not be *prosecuted*—the proffered defenses are unavailable for numerous Internet content providers. The Government suggests that content providers should "tag" their material, but recognizes that the effectiveness of tagging depends wholly on the actions of third parties—manufacturers of client software—on whom the Act places no obligations whatsoever. The Government also suggests that registration with the "marketplace of browsing and blocking software" will constitute "substantial evidence" of good faith, despite the fact that the effectiveness of such steps depends on the availability and use of services that offer to block sites, browsers that have screening capabilities, or blocking software. (*See* Defendant's Post-Hearing Memo. at 44-45) In the absence of evidence that the marketplace actually offers a substantial number of services and products with

blocking capabilities—and, indeed, in the face of evidence that households do *not* tend to use existing parental control software, *see* findings of fact, *supra*, at p. 929—the Government's position is untenable. We have no doubt that, under current technology, the availability of a good-faith defense in § 223(e)(5)(A) will not lessen the chill on protected expression created by § 223(d) of the CDA. (*See* Oral Argument, June 3, 1996, Tr. at 18)

The Government urges that we overlook the fact that the standards and client software necessary to ensure that content providers can enter § 223(e)(5)(A)'s safe harbor are not currently in place, and that we trust that standards and technology will evolve rapidly in response to the CDA. The Government thus argues that a defense to criminal liability under a statute regulating constitutionally protected speech is not now available but will be in short order. We decline to accept such an argument. We cannot uphold a statute against a First Amendment challenge in the uncertain expectation that future technology will remedy any constitutional infirmities. Even if we could be certain that technological advancement would rapidly render the good-faith defense practicable, we necessarily decide questions of law in the factual context of the world as we know it, mindful that restrictions on First Amendment freedoms, "for even minimal periods of time, unquestionably constitute[ ] irreparable injury." *Elrod*, 427 U.S. at 373, 96 S.Ct. at 2689.

Section 223(e)(5)(A) offers the only possible defense for those who wish to communicate by e-mail, newsgroups, or chat rooms or those who choose to make files available by running an FTP or gopher

server. In addition, it offers the only defense for non-commercial—and possibly some commercial-content providers of World Wide Web material. The fact that § 223(e)(5)(B) may offer a defense to Web providers who primarily make content available for purchase leads the Government to urge that, at a minimum, we uphold § 223(d) as to commercial providers of Web content.[20]

We recognize that courts should attempt to limit a statute's scope before resolving to declare it facially void. Two roads are available in this respect; a court can strike a portion of a statutory provision, leaving the remainder of the legislation intact, or it can leave the law's language in place but assign to it a narrow meaning. However, the circumstances here presented do not permit us either of these options to save part, if not all, of the statute.

The Supreme Court has repeatedly recognized the " 'elementary principle that the same statute may be in part constitutional and in part unconstitutional, and that if the parts are wholly independent of each other, that which is constitutional may stand while that which is unconstitutional will be rejected.' " *Brockett v. Spokane Arcades, Inc.*, 472 U.S. 491, 502, 105 S.Ct. 2794, 2801, 86 L.Ed.2d 394 (1985) (quoting *Allen v. Louisiana*, 103 U.S. (13 OHO) 80, 83-84, 26 L.Ed. 318 (1881)). Where it is possible to identify in the text of a statute particular language that is

---

[20] We note that in *ACLU/ALA*, the Government apparently urged an even narrower approach—namely, that the Court uphold the statute as to commercial purveyors of pornography. *See ACLU/ALA*, 929 F.Supp. at 854 (Sloviter, C.J.); *cf.* Oral Argument, *Shea v. Reno*, June 3, 1996, Tr. at 74-75.

unconstitutional, a court should attempt to strike only that language, provided that the remainder of the statute can function effectively without the excised portion and that the resulting whole is consistent with the intent and design of Congress. *Alaska Airlines, Inc. v. Brock*, 480 U.S. 678, 684-85, 107 S.Ct. 1476, 1479-80, 94 L.Ed.2d 661 (1987). Thus, for example, in *Brockett*, the Court reversed the appellate court's facial invalidation of Washington's moral nuisance statute, finding that the statute could survive a First Amendment attack if, at worst, the word "lust" were struck from its definitional section. 472 U.S. at 504-07, 105 S.Ct. at 2802-03; *see also Alaska Airlines, Inc.*, 480 U.S. at 697, 107 S.Ct. at 1476 (striking down statute's legislative veto component only).

The statute at issue in the instant case, however, nowhere distinguishes between categories of content providers. Even if we were to accept the Government's position that the statute could be constitutionally applied to commercial providers of indecent material, we are not in a position to excise particular statutory language in an effort to salvage the provision, because we cannot identify a "wholly independent" portion of the law that can be described as constitutionally infirm.

Nor would it be appropriate for the Court to assign a narrow construction to the statute's existing language. Although we recognize that this is the proper approach in many instances, *see, e.g., National Advertising Co. v. City of Orange*, 861 F.2d 246 (9th Cir.1988) (construing Orange City anti-billboard ordinance to apply only to commercial billboards); *Doyle v. Suffolk County*, 786 F.2d 523 (2d Cir.) (saving New

York law from invalidity under ADEA by exempting individuals aged forty to seventy from its prohibition on applicants over age twenty-nine), *cert. denied*, 479 U.S. 825, 107 S.Ct. 98, 93 L.Ed.2d 49 (1986), there are limits on the extent to which the courts can salvage legislation through limiting interpretation. A statutory provision must be "easily susceptible of a narrowing construction." *Erznoznik v. City of Jacksonville*, 422 U.S. 205, 216, 95 S.Ct. 2268, 2276, 45 L.Ed.2d 125 (1975) (declining to construe city ordinance narrowly to avoid First Amendment facial invalidation); *See Virginia v. American Booksellers Ass'n*, 484 U.S. 383, 397, 108 S.Ct. 636, 645, 98 L.Ed.2d 782 (1988) (dicta) (noting that "the statute must be 'readily susceptible' to the limitation; we will not rewrite a state law to conform it to constitutional requirements"). Otherwise, the courts risk intrusion into the legislative sphere. *See United States v. National Treasury Employees Union*, — U.S. ——, ——, 115 S.Ct. 1003, 1019, 130 L.Ed.2d 964 (1995) (declining to read nexus requirement into Ethics in Government Act, noting its "obligation to avoid judicial legislation" and concluding, "We cannot be sure that our attempt to redraft the statute . . . would correctly identify the nexus Congress would have adopted . . . .").

In the instant case, we would need to limit the statutory term "any person" to mean "any commercial content provider," or, possibly, "any commercial provider of Web content," or even "any commercial purveyor of pornography on the World Wide Web." The statute is far from "readily susceptible" to any such limitation. Rather, any such interpretation would fly in the face of a clear

congressional intent to apply the statute's proscriptions to commercial and non-commercial content providers alike. *See* S.CONF.REP. No. 230, 104th Cong., 2d Sess. 191 (1996). The construction of the statute urged by the Government here would require the court to substantially redraft the statute—in effect, to usurp Congress's legislative functions. We cannot accept the invitation to so reconfigure this statute and thus engage in judicial legislation—the very "judicial legislation" that the Supreme Court condemned in *National Treasury Employees Union.*

Nor does the statute at issue in the instant case lend itself to a gradual narrowing through case-by-case adjudication along the lines of the Supreme Court's approach in *Broadrick*, 413 U.S. at 601, 93 S.Ct. at 2908. In *Broadrick*, the Court limited its holding to the parties before it in the express expectation that subsequent cases would serve to define the statute's proper scope. It did so, however, recognizing that the potential range of the law's unconstitutional applications was not "substantial . . . in relation to the statute's plainly legitimate sweep." *Id.* at 616, 93 S.Ct. at 2918; *see also New York v. Ferber*, 458 U.S. 747, 773-74, 102 S.Ct. 3348, 3363-64, 73 L.Ed.2d 1113 (1982). In the instant case, the evidence suggests that the set of content providers whose speech could be constitutionally proscribed is in fact exceeded, perhaps even overshadowed, by the number of users whose speech is constitutionally protected. Under these circumstances, this Court may not leave to subsequent adjudication the task of defining the potentially expansive set of users who should be outside the statute's scope.

CONCLUSION

To summarize, we find as follows:

(1) The plaintiff has not demonstrated a likelihood of success on his claim that § 223(d) is void as unconstitutionally vague.

(2) The plaintiff has demonstrated a likelihood of success on the merits of his second substantial overbreadth claim, that § 223(d) serves as a ban on constitutionally protected indecent communication between adults;

(a) The Government has conceded that § 223(d), standing alone, is unconstitutional as a total ban on protected indecent communication between adults;

(b) Current technology provides no feasible means for most content providers to avail themselves of the two affirmative defenses to § 223(d) set out in § 223(e)(5).

Accordingly, the plaintiff's Motion for a Preliminary Injunction (filed Feb. 17, 1996) is granted: the defendant is preliminarily enjoined, until further order of this Court, from initiating any investigation or prosecution under § 223(d), to the extent that such investigation or prosecution is based upon the alleged display or transmission of indecent but not obscene material.

It is so ordered.

APPENDIX B

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

No. 96 Civ. 0976 (DLC)

JOE SHEA, ON BEHALF OF THE AMERICAN REPORTER, PLAINTIFF

v.

JANET M. RENO, ATTORNEY GENERAL OF THE UNITED STATES OF AMERICA, DEFENDANT

[Filed: Aug. 15, 1996]

NOTICE OF APPEAL

Notice is hereby given that defendant Janet M. Reno, in her official capacity as Attorney General of the United States, hereby appeals, pursuant to section 561(b) of the Telecommunications Act of 1996, Pub. L. No. 104-104, § 561(b), 110 Stat. 143, to the Supreme Court of the United States from the Opinion and Order entered July 29, 1996 granting plaintiff's motion for preliminary injuction.

MARY JO WHITE
United States Attorney for the
Southern District of New York
Attorney for Defendant

By: /s/ WILLIAM HOFFMAN
WILLIAM J. HOFFMAN (WH-3792)
Assistant United States Attorney
100 Church Street, 19th Floor
New York, New York 10007
(212) 385-6250

APPENDIX C

STATUTORY PROVISIONS

Title V of the Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 133, provides in part:

TITLE V—OBSCENITY AND VIOLENCE

Subtitle A—Obscene, Harassing, and Wrongful Utilization of Telecommunications Facilities

SEC. 501. SHORT TITLE.

This title may be cited as the "Communications Decency Act of 1996".

SEC. 502. OBSCENE OR HARASSING USE OF TELECOMMUNICATIONS FACILITIES UNDER THE COMMUNICATIONS ACT OF 1934.

Section 223 (47 U.S.C. 223) is amended—

(1) by striking subsection (a) and inserting in lieu thereof:

"(a) Whoever—

"(1) in interstate or foreign communications—

"(A) by means of a telecommunications device knowingly—

"(i) makes, creates, or solicits, and

"(ii) initiates the transmission of,

any comment, request, suggestion, proposal, image, or other communication which is obscene, lewd, lascivious, filthy, or indecent, with intent to annoy, abuse, threaten, or harass another person;

"(B) by means of a telecommunications device knowingly—

"(i) makes, creates, or solicits, and

"(ii) initiates the transmission of,

any comment, request, suggestion, proposal, image, or other communication which is obscene or indecent, knowing that the recipient of the communication is under 18 years of age, regardless of whether the maker of such communication placed the call or initiated the communication;

"(C) makes a telephone call or utilizes a telecommunications device, whether or not conversation or communication ensues, without disclosing his identity and with intent to annoy, abuse, threaten, or harass any person at the called number or who receives the communications;

"(D) makes or causes the telephone of another repeatedly or continuously to ring, with intent to harass any person at the called number; or

"(E) makes repeated telephone calls or repeatedly initiates communication with a telecommunications device, during which conversation or communication ensues, solely to

harass any person at the called number or who receives the communication; or

"(2) knowingly permits any telecommunications facility under his control to be used for any activity prohibited by paragraph (1) with the intent that it be used for such activity,

shall be fined under title 18, United States Code, or imprisoned not more than two years, or both."; and

(2) by adding at the end the following new subsections:

"(d) Whoever—

"(1) in interstate or foreign communications knowingly—

"(A) uses an interactive computer service to send to a specific person or persons under 18 years of age, or

"(B) uses any interactive computer service to display in a manner available to a person under 18 years of age,

any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs, regardless of whether the user of such service placed the call or initiated the communication; or

"(2) knowingly permits any telecommunications facility under such person's control to be used for an activity prohibited by paragraph (1) with the intent that it be used for such activity,

shall be fined under title 18, United States Code, or imprisoned not more than two years, or both.

"(e) In addition to any other defenses available by law:

"(1) No person shall be held to have violated subsection (a) or (d) solely for providing access or connection to or from a facility, system, or network not under that person's control, including transmission, downloading, intermediate storage, access software, or other related capabilities that are incidental to providing such access or connection that does not include the creation of the content of the communication.

"(2) The defenses provided by paragraph (1) of this subsection shall not be applicable to a person who is a conspirator with an entity actively involved in the creation or knowing distribution of communications that violate this section, or who knowingly advertises the availability of such communications.

"(3) The defenses provided in paragraph (1) of this subsection shall not be applicable to a person who provides access or connection to a facility, system, or network engaged in the violation of this section that is owned or controlled by such person.

"(4) No employer shall be held liable under this section for the actions of an employee or agent unless the employee's or agent's conduct is within the scope of his or her employment or agency and the employer (A) having knowledge of such con-

duct, authorizes or ratifies such conduct, or (B) recklessly disregards such conduct.

"(5) It is a defense to a prosecution under subsection (a)(1)(B) or (d), or under subsection (a)(2) with respect to the use of a facility for an activity under subsection (a)(1)(B) that a person—

"(A) has taken, in good faith, reasonable, effective, and appropriate actions under the circumstances to restrict or prevent access by minors to a communication specified in such subsections, which may involve any appropriate measures to restrict minors from such communications, including any method which is feasible under available technology; or

"(B) has restricted access to such communication by requiring use of a verified credit card, debit account, adult access code, or adult personal identification number.

"(6) The Commission may describe measures which are reasonable, effective, and appropriate to restrict access to prohibited communications under subsection (d). Nothing in this section authorizes the Commission to enforce, or is intended to provide the Commission with the authority to approve, sanction, or permit, the use of such measures. The Commission shall have no enforcement authority over the failure to utilize such measures. The Commission shall not endorse specific products relating to such measures. The use of such measures shall be admitted as evidence of good faith efforts for purposes of paragraph (5) in any action arising under subsection (d). Nothing in

this section shall be construed to treat interactive computer services as common carriers or telecommunications carriers.

"(f)(1) No cause of action may be brought in any court or administrative agency against any person on account of any activity that is not in violation of any law punishable by criminal or civil penalty, and that the person has taken in good faith to implement a defense authorized under this section or otherwise to restrict or prevent the transmission of, or access to, a communication specified in this section.

"(2) No State or local government may impose any liability for commercial activities or actions by commercial entities, nonprofit libraries, or institutions of higher education in connection with an activity or action described in subsection (a)(2) or (d) that is inconsistent with the treatment of those activities or actions under this section: *Provided, however*, That nothing herein shall preclude any State or local government from enacting and enforcing complementary oversight, liability, and regulatory systems, procedures, and requirements, so long as such systems, procedures, and requirements govern only intrastate services and do not result in the imposition of inconsistent rights, duties or obligations on the provision of interstate services. Nothing in this subsection shall preclude any State or local government from governing conduct not covered by this section.

"(g) Nothing in subsection (a), (d), (e), or (f) or in the defenses to prosecution under subsection (a) or (d) shall be construed to affect or limit the application or enforcement of any other Federal law.

"(h) For purposes of this section—

"(1) The use of the term 'telecommunications device' in this section—

"(A) shall not impose new obligations on broadcasting station licensees and cable operators covered by obscenity and indecency provisions elsewhere in this Act; and

"(B) does not include an interactive computer service.

"(2) The term 'interactive computer service' has the meaning provided in section 230(e)(2).

"(3) The term 'access software' means software (including client or server software) or enabling tools that do not create or provide the content of the communication but that allow a user to do any one or more of the following:

"(A) filter, screen, allow, or disallow content;

"(B) pick, choose, analyze, or digest content; or

"(C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content.

"(4) The term 'institution of higher education' has the meaning provided in section 1201 of the Higher Education Act of 1965 (20 U.S.C. 1141).

"(5) The term 'library' means a library eligible for participation in State-based plans for funds under title III of the Library Services and Construction Act (20 U.S.C. 355e et seq.).".

* * * * *